Mark Minasi's Windows Power Tools p. 9

Windows IT Pro

A PENTON PUBLICATION

DECEMBER 2011 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU



OUR PICKS! BEST PRODUCTS OF 2011 YOUR PICKS!

Editors' Choice and Community Choice Winners p. 23

Windows Server 2008 R2 Firewall Security p. 53

Configure Outlook 2010 Protection Rules p. 57

Find Special Folder Paths with PowerShell p. 64

Windows 8 Sneak Peek p. 40

Master Site Topology for Active Directory Replication p. 44

Digital Edition Copyright Notice

The content contained in this digital edition ("Digital Material"), as well as its selection and arrangement, is owned by Penton Media, Inc. and its affiliated companies, licensors, and suppliers, and is protected by their respective copyright, trademark and other proprietary rights.

Upon payment of the subscription price, if applicable, you are hereby authorized to view, download, copy, and print Digital Material solely for your own personal, non-commercial use, provided that by doing any of the foregoing, you acknowledge that (i) you do not and will not acquire any ownership rights of any kind in the Digital Material or any portion thereof, (ii) you must preserve all copyright and other proprietary notices included in any downloaded Digital Material, and (iii) you must comply in all respects with the use restrictions set forth below and in the Penton Privacy Policy and the Penton Terms of Use (the "Use Restrictions"), each of which is hereby incorporated by reference. Any use not in accordance with, and any failure to comply fully with, the Use Restrictions is expressly prohibited by law, and may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum possible extent.

You may not modify, publish, license, transmit (including by way of email, facsimile or other electronic means), transfer, sell, reproduce (including by copying or posting on any network computer), create derivative works from, display, store, or in any way exploit, broadcast, disseminate or distribute, in any format or media of any kind, any of the Digital Material, in whole or in part, without the express prior written consent of Penton Media, Inc. To request content for commercial use or Penton's approval of any other restricted activity described above, please contact the Reprints Department at (888) 858-8851. Without in any way limiting the foregoing, you may not use spiders, robots, data mining techniques or other automated techniques to catalog, download or otherwise reproduce, store or distribute any Digital Material.

NEITHER PENTON NOR ANY THIRD PARTY CONTENT PROVIDER OR THEIR AGENTS SHALL BE LIABLE FOR ANY ACT, DIRECT OR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR ACCESS TO ANY DIGITAL MATERIAL, AND/OR ANY INFORMATION CONTAINED THEREIN.



DB2 on POWER: 3x faster. Check. As low as 1/3 the price. Mate.

Which database has the right moves? DB2® on Power Systems™ performs three times faster per core than Oracle Database on SPARC—based on both TPC-C and SAP® SD benchmarks.* Yet the price of DB2 is as low as 1/3 the price of Oracle Database.** Maybe that's why in 2010 over 1,000 Oracle Database clients chose DB2 instead. Game over.

ibm.com/facts

*PERFORMANCE: www.tpc.org as of 3/28/11 [IBM Power 780 (3 x 64 C)(24 Ch/192 C/768 Th); 10,366,254 tpmC; $1.38/tpmC; avail. 10/13/10 v. Oracle SPARC SuperCluster w/T3–4 Servers (27 x 64 C)(108 Ch/1728 C/13824 Th); 30,249,688 tpmC; $1.01/tpmC; avail. 6/1/11]. TPC-C is a trademark of Transaction Performance Processing Council. 2-tier SAP SD standard application benchmark results as of 3/28/11 [IBM Power 795 (32 P/256 C/1024 Th); 126,063 users, SAP ERP 6.0 EhP4/AIX 7.1 + DB2 9.7; cert. 2010046 v. Oracle SPARC Enterprise Server M9000 (64 P/256 C/512 Th); 39,100 users, SAP ERP 6.0/Solaris 10, Oracle 10g; cert. 2008042] www.sap.com/benchmark. SAP and all SAP logos are trademarks or registered trademarks of SAP AG in Germany and several other countries. **PRICE: based on publicly avail. U.S. info on 2/10/2011 for IBM DB2 Advanced Enterprise Edition + Oracle software w/comparable capabilities. No SAP SD benchmark results are used for any price/performance metrics. IBM: 100 Processor Value Units. Oracle: assumes 1.0 processor multiplier. Both incl. Y1 maint./support. IBM, the IBM logo, ibm.com, DB2, Power Systems, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. © International Business Machines Corporation 2011.

CONTENTS



COVER STORY

23 2011 *Windows IT Pro* Editors' Best & Community Choice Awards
The polls have closed! Here are your—and our—favorite products of the year.
BY *WINDOWS IT PRO* EDITORS

FEATURES

40 Windows 8: A Sneak Peek at Microsoft's Newest Client OS
Microsoft claims that Windows 8 is "Windows reimagined"—and Windows 8 is indeed a fresh new start for Windows, for both users and developers.
BY PAUL THURROTT

44 Active Directory Replication Topology
A site topology consists of sites, site links, and site link bridges that generally map closely to the network topology. Understanding how to build a site topology is essential for your Active Directory to replicate efficiently and fail over gracefully in case of a network outage.
BY BRIAN DESMOND

53 Windows Server 2008 R2 Firewall Security
Windows Server 2008 R2 and Windows Server 2008 are the first versions of Windows Server in which you can successfully keep your firewall enabled and still have the server work in a production environment. The Microsoft Management Console (MMC) *Firewall with Advanced Security* snap-in is key to this capability.
BY ALAN SUGANO

57 Outlook 2010 Protection Rules
New features in Microsoft Outlook 2010 let you expand data protection. Learn how to configure your servers and end-user systems to take advantage of these features.
BY JOHN HOWIE

64 Easily Find Special Folder Paths with PowerShell
Paths to key OS and user folders aren't always standardized. Here's a way to reliably find and use them in your PowerShell scripts.
BY ALEX K. ANGELOPOULOS

67 Wi-Fi Best Practices
Learn some common-sense best practices related to radio spectrum bands, channel selection, and security that you can implement to enhance the security, reliability, and availability of your Wi-Fi setup.
BY MICHAEL DRAGONE

72 Unleash the Power of Windows Phone
Application support for Windows Phone was significantly improved leading up to the release of Windows Phone 7.5. Even using only free apps, you can greatly enhance Windows Phone's capabilities.
BY DAMIR DIZDAREVIC

75 SharePoint 2010 Goes Social, Part 3
Kevin Laahs concludes his series on social networking with SharePoint Server 2010 by describing the major features that build on the user profile to leverage an often forgotten information source—people.
BY KEVIN LAAHS

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the Search box on the home page.

Windows IT Pro
A PENTON PUBLICATION
DECEMBER 2011
VOLUME_17 NO_12

COLUMNS

OTEY | IT PRO PERSPECTIVES



4 Server Management in Windows Server 8
Server management moves off of the desktop and away from the GUI, into the command line—letting you manage multiple servers from one dashboard.

THURROTT | NEED TO KNOW



7 The Windows 8 Paradox, A Mobile Market Reshuffle, and RIM's Nosedive Into Obscurity
Windows 8 Developer Preview is incomplete—for now—creating a paradox for power users. Plus, how the mobile market could shift to put Windows Phone ahead of the iPhone. And where is RIM's road map?

MINASI | WINDOWS POWER TOOLS



9 Digging Deeper into Get-ADUser
Now that he's presented some Get-ADUser basics, Mark dives further into the tool to see how to get the most out of PowerShell Active Directory queries.

OTEY | TOP 10



10 New Features in Windows Server 8
With huge improvements to its virtualization, management, and PowerShell support, Window Server 8 is one of the biggest server releases Microsoft has ever produced.

DEUBY | ENTERPRISE IDENTITY



12 NSTIC Lays Out a Compelling Identity-Ecosystem Vision
The National Strategy for Trusted Identities in Cyberspace (NSTIC) has a vision for the future: an Identity Ecosystem in which everyone enjoys greater trust and security as they conduct sensitive transactions online.

CONTENTS

PRODUCTS

82 New & Improved
Check out the latest products to hit the marketplace.
PRODUCT SPOTLIGHT: **up.time software**.

REVIEW
83 Paul's Picks
What's to like about Windows Phone 7.5, and why iPhone 4 owners won't flock to iPhone 4S.
BY PAUL THURROTT

84 Industry Bytes
Jason Bovberg outlines the top 10 reasons SMBs fail to back up their data, Tony Redmond discusses why Exchange administrators should embrace PowerShell, and B.K. Winstead explains why organizations should include mobile device management in their policies.

INTERACT

16 Reader to Reader
By deploying Microsoft System Center Data Protection Manager 2010 on a dedicated backup network, you'll have a tool that will protect your data without clogging up your production network with extra traffic.

20 Ask the Experts
Learn more about Windows 8, find out the exact roles of a Windows account's SID, and get your VMware questions answered.

IN EVERY ISSUE



87 Directory of Services
87 Advertising Index
87 Vendor Directory
88 Ctrl+Alt+Del

Windows IT Pro

EDITORIAL

Editor in Chief
Amy Eisenberg amy@windowsitpro.com

Senior Technical Director
Michael Otey motey@windowsitpro.com

Technical Director
Sean Deuby sean@windowsitpro.com

Senior Technical Analyst
Paul Thurrott paul@windowsitpro.com

Industry News Analyst
Jeff James jjames@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Exchange & Outlook
Brian Winstead bwinstead@windowsitpro.com

Systems Management, Networking, Hardware
Jason Bovberg jbovberg@windowsitpro.com

Security, Virtualization
Jeff James jjames@windowsitpro.com

SharePoint
Caroline Marwitz cmarwitz@windowsitpro.com

SQL Server, Developer Content
Megan Keller mkeller@windowsitpro.com

Managing Editor
Lavon Peters lavon.peters@penton.com

Editorial Assistant
Blair Greenwood blair.greenwood@penton.com

CONTRIBUTORS

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com
John Savill john@savilltech.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond 12knocksinna@gmail.com
Eric B. Rux ericbrux@whshelp.com
William Sheldon bsheldon@interknowlogy.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Graphic Designer
Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com

Director of IT Strategy and Partner Alliances
Birdie J. Ghiglione birdie.ghiglione@penton.com
619-442-4064

Online Sales Development Director
Amanda Phillips amanda.phillips@penton.com

Key Account Director
Chrissy Ferraro christina.ferraro@penton.com
970-203-2883

Account Executives
Barbara Ritter barbara.ritter@penton.com
858-367-8058
Cass Schulz cassandra.schulz@penton.com
858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

IT Group Audience Development Director
Marie Evans marie.evans@penton.com

Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

PENTON

Chief Executive Officer
Sharon Rowlands sharon.rowlands@penton.com

Chief Financial Officer/Executive Vice President
Nicola Allais nicola.allais@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

Windows®, Windows Vista®, and Windows Server® are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries and are used by Penton Media under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation.

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

PROGRAM CODE
Unless otherwise noted, all programming code in this issue is © 2011, Penton Media, Inc., all rights reserved. These programs may not be reproduced or distributed in any form without permission in writing from the publisher. It is the reader's responsibility to ensure procedures and techniques used from this publication are accurate and appropriate for the user's installation. No warranty is implied or expressed.

LIST RENTALS
Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

REPRINTS
Wright's Media
penton@wrightsmedia.com 877-652-5295

Make Your Mark with SharePoint Branding

Free Virtual Conference

December 7th

Join experts Celina Baginski, Colin Spence, Randy Williams, and others for a series of free technical sessions for developers and administrators that will help you get the most value from SharePoint.



Celina Baginski



Colin Spence



Randy Williams

Go to sharepointpromag.com/events to register!



Otey

"Windows Server 8 takes these practical task-oriented tools in Server Manager and extends their reach out to all the networked servers in your organization."

Server Management in Windows Server 8

Windows management evolves from single server to multi-server

Windows Server 8 promises to be one of the most significant releases of the OS to date. Despite the glut of new features, one of the biggest changes is more subtle—Windows Server 8 marks a change in mindset for the way Windows servers should be run and managed. With Windows Server 8, server management moves off of the desktop and away from the GUI into the command line. At the same time, there's a corresponding move from single-server management to managing all of your servers as a whole.

Server Core Is the New Default

The first change that really signifies Microsoft's new attitude toward server management is the fact that the default installation type for Windows Server 8 will be in the Server Core mode. The advantages to Server Core and headless server management include less patching and improved security, thanks to a reduced footprint and code base.

Server Core has been available since Windows Server 2008. However, it hasn't caught on because Server Core is just too difficult to manage. I remember attempting to set up a Hyper-V Server Core system only to find out I needed to go through 27 (I'm not kidding) manual configuration steps, and, in the end, it still didn't work. I wound up reinstalling the server using the full installation just to get on with things.

Microsoft revamped both remote management in Windows Server 8 and how Windows Server can switch between the Server Core installation and the full GUI. Server 8 remote management won't rely on DCOM as Windows Server 2008 did. And the GUI will be a feature that can be installed and uninstalled.

This approach will let you install and initially configure a server using the GUI and then pull the GUI off before commencing day-to-day operations. There's no need to reinstall the OS like there is today. SQL Server, another important Windows infrastructure technology, will also be supported under Server Core.

Multi-Server Management Is Built In

Windows Server 2008 R2 and earlier releases all focus on single-system management. The Windows Server 2008 Server Manager tool is far better than any of the previous versions. However, although the Server Manager provides a useful and practical management dashboard, the tool is primarily oriented toward managing the local server.

Windows Server 8 takes these practical task-oriented tools in Server Manager and extends their reach out to all the networked servers in your organization. The new Windows Server 8 Server Manager lets you create groups of multiple servers, and the actions available in the Server Manager can be applied to all the servers from a single management dashboard.

In addition, you can connect to remote servers and drill down into their management details much like managing local servers today. Remote multi-server management becomes especially important when servers in the enterprise are running headless with no local graphical management interface.

PowerShell Will Be the New Management Standard

True headless Windows servers and multi-server management are sure to be welcomed with open arms. However, PowerShell will be a tougher sell to administrators. Although Microsoft has definitely lined up behind PowerShell, most administrators haven't.

Microsoft has been gradually building PowerShell management into all of its server products. PowerShell is powerful, but it's also complex. In the case of Windows Server management, PowerShell has also always been limited. Currently, there are too many cases in which you need to drop back to Windows Command Shell, Netsh, or VBScript and Windows Management Instrumentation (WMI) to get things done.

With Windows Server 8, Microsoft has really addressed the breadth of tasks that PowerShell can tackle. Probably the most notable change is the fact that Microsoft has increased the number of built-in cmdlets from about 200 to about 2,300. The Integrated Scripting Environment (ISE) has also been enhanced. For Windows administrators, this is definitely a heads-up that it's time to learn more about Windows management using PowerShell.

Managing Servers as Infrastructure

With Windows Server 8, Microsoft really has moved server management off of the desktop and into the infrastructure where servers will be managed as servers. I'm convinced that this is the right direction—particularly when you see servers as background infrastructure components that are providing services to a dynamic IT infrastructure and to the private cloud.

InstantDoc ID 140938

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).



Thinking about migrating to System z? You're in good company.

Since the start of 2010, more than 250 companies around the world have migrated workloads (including Oracle® workloads) to System z®. Why? Maybe it's the savings (up to 50% on applicable IT costs). Or the top-rated EAL5 security classification. Or because it delivers up to 99.999% availability and uptime. Or maybe it's an even better reason: all of the above.

ibm.com/facts

IT COST SAVINGS reflect overall reductions in software and/or hardware maintenance charges and reduced costs of system and workload management over a period of 3–5 years, when consolidating workloads from other systems to a virtualized Linux environment on System z. AVAILABILITY percentage is based on System z servers in a Parallel Sysplex environment, assuming application data sharing across multiple servers. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions. Contact IBM to see what we can do for you. Current as of 7/7/2011. IBM, the IBM logo, ibm.com, System z, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. © International Business Machines Corporation 2011.

CLOUD CONNECTIONS

WINDOWS CONNECTIONS

Microsoft® Exchange CONNECTIONS

UNIFIED COMMUNICATIONS CONNECTIONS

EXCHANGE MANAGEMENT SHELL

LYNC

OFFICE 365

WINDOWS INTUNE

VIRTUALIZATION

BI SEMANTIC MODEL

SYSTEM CENTER VIRTUAL MACHINE MANAGER

SYSTEM CENTER ORCHESTRATOR

SQL SERVER 2012

SQL AZURE

EXCHANGE ONLINE

WINDOWS 8

SHAREPOINT

DAGs

WINDOWS SERVER 2008 R2 SP1

KEYNOTE SPEAKERS



MARK MINASI
MINASI RESEARCH AND DEVELOPMENT



PAUL THURROTT
WINDOWS IT PRO NEWS EDITOR



SEAN DEUBY
PENTON MEDIA



KIMBERLY L. TRIPP
SQLSKILLS.COM



PAUL S. RANDAL
SQLSKILLS.COM



Take the Journey into 2012 with Microsoft & Industry Experts as New Technologies & Products Launch

- TRAIN WITH 100+ MICROSOFT & INDUSTRY EXPERTS
- OVER 250 IN-DEPTH SESSIONS
- EXCITING NETWORKING PARTY OPPORTUNITIES

CO-LOCATED WITH

Microsoft® SQL Server®

MAR. 26 - 29, 2012
LAS VEGAS, NV
MGM GRAND

2012 LAUNCH

powered by Microsoft® & SQL Server CONNECTIONS

REGISTER TODAY! www.WinConnections.com • 800.438.6720 • 203.400.6121

Thurrott



"I think Windows Phone needs some outside help, something akin to the asteroid that killed off the dinosaurs, an unforeseen bit of good news. That good news might be Apple's recently released iPhone 4S."

The Windows 8 Paradox, A Mobile Market Reshuffle, and RIM's Nosedive Into Obscurity

As we head into the end of 2011, questions remain about Windows 8 and Windows Phone. And the answers to those questions aren't necessarily what you were expecting. As I write this, it's been over a month since Microsoft unveiled Windows 8 at its epic BUILD Conference in Anaheim, California. Since then, I've tried to spend as much time as I can in the new OS, not just via the Samsung tablet that Microsoft loaned me at the show, but on as many of my own PCs as possible.

The Windows 8 Paradox

It's been a bit difficult, frankly. And the difficulties I'm seeing are echoed in a growing cacophony of online complaints from power users around the world.

They're all very misguided.

Here's why: When Microsoft shipped the Windows 8 Developer Preview in September, it did so to provide developers with a way to start investigating the new Windows runtime, WinRT, and the new Metro-style apps that they could create for this environment. But the Developer Preview isn't complete. Yes, it ships with a variety of intern-created sample apps, but all of those are fairly basic, leading to unwarranted criticism that this new environment, as denoted by the Windows 8 Start screen and the apps that run within, is a sort of overly simplistic experience, and that the computing world of the future will be defined by a two-tier user experience: The Fisher-Price world of the Start screen and the more powerful and refined world of the legacy Windows desktop.

Folks, it's not true. As Microsoft has explained—but, admittedly, not ably demonstrated—WinRT is a fully capable and rich app environment that lends itself equally well to complex applications such as Microsoft Office, Adobe Photoshop, and modern 3D video games, as it does to simple weather and Twitter apps. The problem is, none of those apps exist today. So people who run the Developer Preview on their own machines are forced to switch back and forth between the future (the Start screen and a handful of simple apps) and the past (the desktop and the huge canon of existing Windows applications). And naturally, they find the future lacking. That's because there aren't any useful apps there.

Yet.

Here's what's going to happen: Microsoft very specifically offered the Windows 8 Developer Preview first so that developers could begin hacking away at the system. And the result is going to be a wellspring of new Metro-style apps that beta testers will be able to download from the Windows Store, which will open in the coming months, well before Windows 8 ships publicly.

(Admittedly, it was also a way to get feedback from the power users who would install this pre-beta build regardless of the warnings. But that need was absolutely secondary: Microsoft is already well aware of the shortcomings of the new environment as it exists in the Developer Preview, and many of the fixes it will implement are already well under way. However, many users will incorrectly assume the company was listening to feedback and fixing issues they found.)

One can logically expect that the Windows 8 user experience will improve by leaps and bounds as Microsoft and numerous third parties race to fill in the gaps between now and the release of Windows 8. Beta testers, with early access to the Windows Store, will be able to download (and buy) numerous Metro-style apps during this time, and as developers get more comfortable with WinRT and its unique abilities, the quality and comprehensiveness of those apps will increase as well. By the time Windows 8 does ship, the store will be well-stocked and developers will be well on their way to mastering the intricacies of this new environment. So users won't be starting with an empty store and a two-tier experience. Many of them will simply use only Metro-style apps and ignore the legacy desktop entirely.

I'm also hearing rumors that some of Microsoft's PC maker partners might ship, in the first half of 2012, tablet computing devices that come with Windows 7 and are compatible with Windows 8. These devices would offer a free Windows 8 upgrade as soon as it's released. This, I think, is a great idea. It lets Microsoft sort-of answer the questions about its delayed response to the iPad, and it provides users with a decent PC tablet experience today with the promise of an excellent Windows 8–based experience just a few months down the road. Will it happen? Stay tuned. I think the Consumer Electronics Show in January 2012 is the ideal time and place to announce such a plan.

Either way, the important thing to note is that the Windows 8 experience of mid-to-late 2012 isn't going to resemble today's experience at all. And while so-called power users continue complaining about the Start screen and the Metro-style apps, it's important to remember that this first Developer Preview isn't for them, it's for developers. And things are going to improve dramatically. Wait for it.

With Lackluster iPhone Upgrade, Hopes for a Mobile Market Reshuffling

Microsoft already makes the best smartphone OS in Windows Phone—it's just that few potential customers realize it. So heading

into the 2011 holiday season, Microsoft and its supporters pinned their hopes on a few things, including the release of Windows Phone 7.5 (excellent, but unlikely to sway the doubters), a new marketing campaign that will provide much-needed incentives to wireless-carrier store employees (so they can temporarily stop mindlessly promoting Android to customers), a handful of new devices from existing partners (none of which, frankly, will make much of a difference), and, of course, everyone's favorite wildcard, Nokia, which promises to unleash a new family of quite excellent Windows Phone 7.5 handsets by the end of the year. (I'll have more on Nokia's offerings next month.)

But then some unexpected help came from an unlikely source: Apple. Now it's possible that everything is about to change.

Stepping back for a moment, let's recall that both Gartner and IDC inexplicably claimed earlier this year that Windows Phone would surpass Apple's iPhone as the number-two smartphone platform behind Google Android by 2012. With Windows Phone languishing in the low single digits from a market-share perspective, these predictions seemed, at the time, laughable. And I argued then, as I do now, that all Microsoft really had to do for the OS to be successful was to establish Windows Phone as one of the top three smartphone platforms. After all, the mobile market is growing at such speed that there's plenty of new users to go around.

But what if Windows Phone really did pull ahead of the iPhone? What would have to happen for such a future to become a reality?

Looking at the list of previously mentioned hopes for the remainder of the year, only one, Nokia's entry into the market, could possibly make a measurable difference to Windows Phone's fortunes. But even Nokia isn't a given, considering how far the company has fallen and how quickly its customer base has jumped ship. In fact, both Gartner and IDC claim that their predictions about Windows Phone are based entirely on Nokia making a huge impact. Which is, of course, why I'm a lot less sanguine about the platform's future than are they.

No, I think Windows Phone needs some outside help, something akin to the asteroid that killed off the dinosaurs, an unforeseen bit of good news that will hobble one of Microsoft's competitors, and thus provide Windows Phone with the opening it needs.

That good news may be Apple's recently released iPhone 4S.

As I write this, the iPhone 4S has garnered supposedly record-breaking sales of 4 million units in its first weekend of availability. And Apple is publicly predicting that it expects to sell 20 million iPhones in the last quarter of 2011, matching its previous, best-ever quarter. But I'd remind people that Apple sells three models of iPhone now, not just the iPhone 4S, but also previous generation (and much cheaper) iPhone 3GS and iPhone 4 handsets. And those older, less expensive phones will almost certainly make up the majority of total iPhone sales in the quarter.

Here's the thing: The iPhone 4S is a great update for iPhone 3GS users, and informal statistics are already showing that these customers—who hit their two-year contract renewal time just as the 4S shipped—do in fact make up the bulk of iPhone 4S buyers. But the iPhone 4S is not a great update for iPhone 4 customers—it utilizes exactly the same form factor as its predecessor, which has to be a turnoff for most—and it's not a great phone for those on other smartphone platforms either, thanks to its small screen and lack of high-end features such as true 4G support.

There's a great chance that the iPhone 4S will end up being something of a letdown for Apple, a device that maintains the status quo at best, and possibly loses share for the platform over the long run. This, of course, would be good news for Microsoft and for Windows Phone, and if Nokia's handsets are as high quality as I believe them to be, it's possible that this lackluster Apple upgrade could drive new users to Windows Phone instead of iPhone.

Is this the perfect storm for Windows Phone? Perhaps, but for this future to unfold as imagined, Microsoft and Nokia are really going to have to step it up, and let's face it, there's little precedent for that. Too, Android, the dominant mobile platform, will likely soak up a lot of potential iPhone customers over the next year, and there's certainly nothing to suggest that Google's aggressive handset partners are going to slow down to accommodate Windows Phone.

Finally, a lackluster upgrade has never stopped Apple from being successful. Apple's ever-broadening fan base has proven that it's always willing and able to open the collective wallet, regardless of the product or the state of the economy. So even the iPhone 4S could end up a success story in its own right. Stranger things have happened.

RIM Continues Its Nosedive Into Obscurity

A few years ago, Nokia owned the worldwide market in the mobile industry with its Symbian OS, and RIM owned the US market, and that for business users, with its BlackBerry system. Today, both of these platforms are in free-fall, with customers abandoning them for the richer ecosystems provided by the Android and the iPhone.

Nokia has moved on and adopted Windows Phone as its smartphone platform, but RIM, well, RIM hasn't had a clear path forward for a while now. It adopted the QNX OS for its Playbook tablet and said that it would use this system for future BlackBerry handsets as well. But at its developer conference in October, the company backpedaled and said it would merge the best of BlackBerry OS and QNX into a new OS called BBX. This will be used for both phones and tablets, though no further details were provided about devices or timing.

In days past, you could argue that the RIM ecosystem made sense because of its security advances over competing systems. But with those differences eroding and no signs of a roadmap, RIM seems to be floundering.

It doesn't help that many BlackBerry users don't actually choose that phone but are provided with it by their employer. Given the choice, many BlackBerry users would jump ship. I certainly would: There are better smartphone platforms out there, including three—Android, iPhone, and Windows Phone—with a much clearer roadmap.



InstantDoc ID 140998

PAUL THURROTT (paul@windowsitpro.com) is the senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows (winsupersite.com), a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email), and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Minasi

"The AD PowerShell team built Get-ADUser parameters for all 100-plus user attributes."



Digging Deeper into Get-ADUser

Get the most out of PowerShell AD queries

In "Find Users with Get-ADUser" (InstantDoc ID 140069), I introduced you to Get-ADUser, a handy Windows Server 2008 R2 Active Directory (AD) cmdlet. This month, I want to dive further into the tool and show you how to get the most out of PowerShell AD queries. Consider this query:

```
get-aduser -f {givenname -like 'M*'}
```

This query returns all users whose first name begins with *M*. Recall that you could've discovered that *givenname* is a legal thing to search on by doing a simpler search and asking PowerShell to reveal the structure of the contents of that search by piping the output to *get-member*, like this:

```
get-aduser -f * -properties * | get-member
```

Then, you might see that you could retrieve all the people whose primary group membership lay with the Domain Admins group with this query, assuming an AD name of bigfirm.com:

```
get-aduser -f {primarygroup -eq 'CN=domain admins,cn=users,
  dc=bigfirm,dc=com'}
```

Here's how I knew that. After running the *get-member* command, I saw a list of the 114 (on my domain) attributes of an AD user, and I noticed a PrimaryGroup attribute. I assumed that I'd have to type it as an LDAP-format name, but I wasn't certain, so I just asked to see it on my user account by using the query we've already seen—but with a more specific *-properties* parameter:

```
get-aduser -f {givenname -eq 'Mark'} -pr PrimaryGroup
```

I got some output that included

```
PrimaryGroup : CN=Domain Users,CN=Users,DC=bigfirm,DC=com
```

And so I saw that forming a query to find the "primary administrator" types would be easy.

By the way, did you notice that I typed *-pr* rather than *-properties*? Recall another sort of shortening that you might have noticed in "Go Remote with Windows Server 2008 R2's AD Cmdlets" (InstantDoc ID 140491). In that article, I said that you could shorten *enter-pssession* to *etsn*. How did I know that? Simple: I used a cmdlet named *get-alias*, which works like so:

```
get-alias -def enter-pssession
```

Alias is PowerShell-ese for "alternate shorter command name that's just as good as the 'official' long name." Try that out for *get-member,* and you'll learn that it has an alias of *gm*. Unfortunately, the AD team didn't assign an alias to Get-ADUser.

The AD PowerShell team did take the time to build Get-ADUser parameters for every one of the 100-plus user attributes (thanks!), so you can even do queries on things as obscure as

```
get-aduser -f {physicaldeliveryofficename -eq 'Downtown'}
```

Take heart in the fact that in that case, the PowerShell AD folks created another parameter, *-office*, that points to the same attribute but involves a bit less typing.

Thus far, we've searched on attributes, but sometimes we're less interested in identifying an AD object via its attributes than we are in identifying the object by its location. For example, suppose one of bigfirm.com's organizational units (OUs) is a geographical one named Pungo, which is one of Bigfirm's offices. Let's also suppose we need to create a query that collects all the AD user objects located in the Pungo OU (in LDAP-ese, *ou=pungo,dc=bigfirm,dc=com*). How do we grab all those folks? I've tried querying on the DistinguishedName of the object, using *-like* to compare it with **ou=pungo,dc=bigfirm,dc=com*, but I didn't get any matches, so it's a good thing we've got the *-searchbase* parameter. Include it and the distinguished name of any container objects in AD in the Get-ADUser command, and you'll restrict the search to just that container. So, for example, to return only the users in Bigfirm's Pungo OU, you could type

```
get-aduser -f * -searchbase "ou=pungo,dc=bigfirm,dc=com"
```

Thus, if we wanted to find everyone in the Pungo OU who has a Gmail account, we could type

```
get-aduser -f {emailaddress -like "*@gmail.com"}
  -searchbase "ou=pungo,dc=bigfirm,dc=com"
```

That's not a bad little query, but PowerShell can do much more complex ones, as you'll see next month.

InstantDoc ID 140932

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books.



Otey

"Microsoft carved out a clear advantage by introducing the ability to perform Live Migration and Storage Live Migration without requiring shared storage."

New Features in Windows Server 8

Get ready for better Hyper-V and cloud-ready management

At this past Windows Server Workshop in Redmond, Washington, Microsoft presented its upcoming version of Windows Server. Window Server 8 is without a doubt one of the biggest server releases Microsoft has ever produced, and the list of enhancements is way too long for one column. Nonetheless, here are my top 10 standout features from Windows Server 8.

1 **Multiserver support in Server Manager**—Windows Server 8 features a completely redesigned Server Manager. Because it embraces the cloud concept, the new Server Manager can manage multiple servers, and it provides an all-new dashboard that lets you drill down into local and remote servers.

2 **Server Core is the default**—Windows Server 8 uses the minimalist Server Core as the default server environment, marking a huge change away from dependence on the GUI for management. The GUI is now considered a feature. Therefore, you can perform your initial server configuration through the GUI, then remove it when you're ready to move into production. Unlike Server 2008 R2, there's no need to reinstall the OS to get rid of the GUI.

3 **Ubiquitous PowerShell management**—Going hand-in-hand with the move away from the GUI is the move to PowerShell as the primary management tool. Windows Server 8 expands the available cmdlets to more than 2,300, providing cmdlets for managing all Windows Server applications. For instance, Server 2008 R2 doesn't have built-in cmdlets for Hyper-V, but Windows Server 8 provides a full set of PowerShell cmdlets for managing Hyper-V 3.0.

4 **Built-in NIC teaming**—Another overdue feature is the capability to provide NIC teaming natively in the OS. VMware's ESX Server has provided NIC teaming for some time. Prior to Windows Server 8, you could get NIC teaming for Windows only via specialized NICs from Broadcom and Intel. The new built-in Windows Server 8 NIC teaming works across heterogeneous vendor NICs and can provide support for load balancing as well as failover over NICs from different vendors.

5 **SMB 2.2**—The Windows Server Message Block (SMB) file sharing protocol has also been significantly enhanced in Windows Server 8. SMB 2.2 adds file server resiliency with no special configuration. In addition, server applications such as Microsoft SQL Server can now have their databases stored on SMB 2.2 shares, which gives them the benefits of SMB 2.2 with no configuration changes to the SQL Server databases.

6 **Data deduplication**—Windows Server 8 provides built-in data deduplication, a feature typically found in high-end SANs. Windows Server 8's data deduplication runs in the background, and it can automatically detect duplicate data, save the duplicated data in a separate system store, and replace the data in the original files with pointers to the system store.

7 **Expanded cluster scalability**—Windows Failover Clustering has also taken a big jump in scalability. VMware's vSphere supported clusters consisting of up to 32 hosts. Previous versions of Windows Server were limited to 16 nodes. Windows Server 8 clusters can support up to 63 nodes and up to 4,000 virtual machines (VMs) per cluster, effectively leap-frogging VMware's VM cluster support.

8 **Multiple concurrent Live Migrations**—Live Migration was introduced with Hyper-V 2.0, which was part of the Server 2008 R2 release. On Hyper-V 2.0, you can perform only one Live Migration at a time. Hyper-V 3.0 brings the ability to perform multiple concurrent Live Migrations to Windows Server 8 and the next release of Hyper-V Server as well.

9 **Storage Live Migration**—The addition of Storage Live Migration to Hyper-V 3.0 really closes the feature gap with VMware. Like VMware's Storage VMotion, Hyper-V 3.0's Storage Live Migration lets you move a VM's virtual disk, configuration, and snapshot files to a new storage location with no interruption of end-user connectivity to the VM.

10 **Live Migration without shared storage**—Unexpectedly, Microsoft really carved out a clear advantage in the small-to-midsized business virtualization market by introducing the ability to perform Live Migration and Storage Live Migration without requiring shared storage on the back end. The ability to perform Live Migration without a SAN back end helps bring the advantages of virtualization and high availability to smaller businesses that can't afford the cost or complexities of a SAN.

InstantDoc ID 140936

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Windows IT Pro Congratulates **PowerWF Studio**

PowerWF™ STUDIO
PowerShell Orchestration

Windows IT Pro 2011 Editors' Best SILVER

Windows IT Pro
Editors' Best Awards

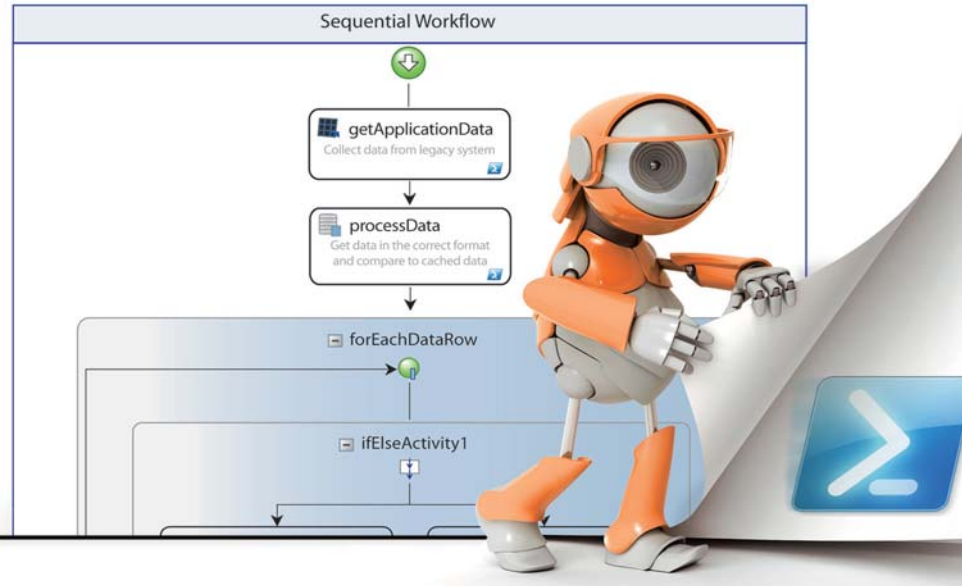
Company: **Devfarm Software**
Category: **Scripting**
Product: **PowerWF Studio**
Award: **Silver**

Learn more about PowerWF here: www.powerwf.com • 314.590.5800

PowerWF™
Workflow Fueled *by* PowerShell

Windows IT Pro 2011 Editors' Best SILVER

PowerShell Orchestration
- THE FUTURE OF IT AUTOMATION -



Visit WWW.POWERWF.COM to download a free trial today.



Deuby

"Jeremy Grant works for the federal government, and he wants to make it easier for you to put sensitive information on the Internet. No, really!"

NSTIC Lays Out a Compelling Identity-Ecosystem Vision

Want a user-centric online environment that celebrates privacy, convenience, efficiency, ease of use, security, innovation, and choice?

Over the past five years, our use of the web for sensitive transactions has grown dramatically. I clearly remember my early orders at Amazon, hesitating at the thought of typing my credit card information on a payment page, worrying that there'd be some technical glitch somewhere between me and the server during processing. (I still have my early-adopter Amazon Bookstore customer gift to prove it!) We've all gotten much more comfortable with e-commerce since then, of course, but there's a very sharp line between what kinds of sensitive transactions you can do online and what kinds you can't (or shouldn't). Many transactions that fall into the "shouldn't" category are there because of the question of identity. It's the essence of the phishing malware attack: Is this person who he says he is? This anonymity, for better or worse, was pointed out in a famous *New Yorker* cartoon in 1993, in which the canine protagonist sitting in front of a computer says to his companion, "On the Internet, nobody knows you're a dog."



If you're reading this column, you're already acutely aware of what's safe to enter and what's not safe. But you're also in the tiny minority. According to the "2011 Identity Fraud Survey Report" by Javelin Strategy & Research (www.identityguard.com/downloads/javelin-2011-identity-fraud-survey-report.pdf), 8.1 million adults were victims of identity theft or fraud, with total costs of $37 billion. Research from Trusteer in 2010 (www.trusteer.com/blog/golden-hour-phishing-attacks) found that phishing attacks continue to increase, and an amazing 50 percent of phishing victims' credentials are harvested by cyber criminals within the first 60 minutes of phishing emails being received.

And passwords just can't cope with the boom. Back in 2004, an RSA working paper found that a small business of 500 employees spends about $110,000 per year on internal password management alone. That's $220 per user per year, and it doesn't account for the costs and risks associated with the explosion in SaaS services since then, most of which require their own user ID and password. We badly need an alternative to passwords. As Jeremy Grant, manager of the National Strategy for Trusted Identities in Cyberspace (NSTIC, pronounced "en-stick" by the cool kids) program office, likes to say, "We think the password is fundamentally insecure and needs to be shot."

Jeremy doesn't just want to make it easier for us to put sensitive information on the Internet. After all, that's the same goal of the phishing messages we're bombarded with on a daily basis. No, Jeremy also wants to make it far more secure for US citizens to conduct all kinds of transactions on the Internet.

NSTIC Vision

The NSTIC program office is part of the National Institute for Standards and Technology (NIST), the people who do everything from keeping track of the fundamental constants of nature (www.nist.gov/pml/div684/constants-071911.cfm) to improving diamond machine polishing techniques (www.nist.gov/pml/div683/nist-polishes-method-for-creating-tiny-diamond-machines.cfm). NSTIC describes "a vision of the future—an Identity Ecosystem—where individuals, businesses, and other organizations enjoy greater trust and security as they conduct sensitive transactions online. The Identity Ecosystem is a user-centric online environment, a set of technologies, policies, and agreed-upon standards that securely support transactions ranging from anonymous to fully authenticated and from low to high value. Key attributes of the Identity Ecosystem include privacy, convenience, efficiency, ease of use, security, confidence, innovation, and choice."

NSTIC isn't a national ID system like the one India is planning (www.governancenow.com/gov-next/egov/govt-planning-multi-use-smart-id-cards-2013); in fact, it's exactly the opposite. No, it's not a devious attempt by the federal government to discover who has assault weapons and take them away in the middle of the night. NSTIC is an acknowledgment that what's needed for secure transactions on the Internet is a common framework that both identity providers (e.g., Google, Facebook, the Department

of Defense—DoD) and service providers (aka relying parties, such as ADP and Dropbox) agree to work within. Because this kind of "co-opitition" can be difficult and time-consuming to achieve, the federal government wants to jumpstart and assist this process as a neutral—but stakeholder—third party. (The government is a stakeholder in this because it is itself one of the world's largest collections of identity providers.) The leaders in developing a national identity ecosystem must be in the private sector, if for no other reason than we wouldn't trust a government system and thus never use it.

NSTIC's envisioned identity ecosystem (www.nist.gov/nstic/identity-ecosystem.html) wouldn't be run by a single identity provider. First, here in the United States, everyone would be suspicious of just one identity provider. Second, consumers want choices and are already associated with a wide variety of identity providers. Unless you're one of the 15 consumers in the United States that hasn't either bought anything from Amazon, logged on to Facebook, or created a webmail account, you already have an identity with a consumer identity provider. You don't need another for a national identity ecosystem.

Instead, NSTIC's vision is to have an online environment where identity providers (both public and private), service providers, and consumers share a set of agreed-upon technologies and standards that create a network supporting trusted IDs that can be used by all parties.

Here's an important point: NSTIC isn't getting into new technology. Secure technologies already exist (e.g., smart cards, digital certificates), so NSTIC is instead focused on policy and standards to ensure that everyone can interoperate with these technologies.

The NSTIC identity ecosystem would allow the consumer to make secure online transactions, with his or her trusted ID, that range from low value and completely anonymous to high value and fully authenticated. This ecosystem would minimize the use of passwords and enable us to do things on the web such as using a smartphone anywhere you'd use a credit card or driver's license today.

From a business standpoint, the NSTIC trusted ID would allow businesses to easily conduct highly secure transactions with each other, minimizing the cybercrime impact that affects so much of e-commerce today. Given a much higher level of security, consumers would be more likely to do their business online, and entirely new classes of e-commerce—such as legal services and online healthcare interactions—would be opened up.

One tenet of this identity ecosystem is that it's voluntary. Identity providers, service providers, and consumers themselves don't have to join. The goal of developing a well-thought-out framework that takes all stakeholders into consideration is to have a *Field of Dreams* model: If you build it, they will come. Consumers will have choices for who they want as an identity provider, and consumer demand will encourage more identity providers and service providers to join the ecosystem. The NSTIC identity ecosystem's benefits will be so compelling for all parties that its adoption will be fueled by its own benefits. As a stakeholder, the government looks to benefit from this framework and is offering its large identity infrastructure to dogfood early implementations as an incentive for deployment.

If you want to have a say in how the identity ecosystem is developed, you should get involved.

NSTIC Ecosystem in Practice

An NSTIC identity ecosystem is far from deployment though; if some of these descriptions sound a bit vague, it's because NSTIC is still in its early stages. The strategy has been published, a national program office for coordinating work has been established, an implementation roadmap has been created, and the deadline for submitting comments on a proposed NSTIC governance structure closed at the end of August.

NSTIC isn't without its challenges. Aaron Titus, chief privacy officer at Identity Finder, is concerned that NSTIC makes privacy a core principle but doesn't recommend regulation to ensure privacy. In other words, regulation must provide the legal stick to the identity ecosystem's carrot to lessen the chance that these powerful new identity credentials will be subject to "hyper-identity theft" if stolen or misused by unscrupulous participants. And getting national legislation passed nowadays, for any reason, is a pretty daunting undertaking. In his blog (www.secureconsulting.net/2011/04/identity-crisis-the-delusion-o.html), Ben Tomhave believes the identity ecosystem is secondary to the number-one identity problem: getting rid of passwords entirely.

It's a vision of how things should be. But as the old proverb says, "The devil's in the details." The private sector must be the entity to step up and figure this out, with a solid governance model that includes a trusted framework between all members. The end result must be trustworthy—not just in the security sense but in the consumer sense. Because if Jim Bob next door or your Aunt Mary doesn't trust it, it won't be adopted. Fortunately, key private-sector identity providers and service providers are commending this effort and getting involved (www.nist.gov/nstic/what-others-are-saying.html).

Get Involved

At the NSTIC launch event, Andrew Nash, director of Internet identity products at Google, stated, "If we don't work out how to move forward from here, the potential of having an Internet that we feel comfortable about using is diminishing rapidly. And that's bad for all of us."

If you're an identity geek or a privacy advocate and you want to have a say in how the identity ecosystem is developed, you should get involved. Go to NSTIC's home page (www.nist.gov/nstic), read the documentation about what NSTIC is (and what it isn't), watch for upcoming notices of inquiry to submit comments and workshops to participate in, or contact Jeremy.

InstantDoc ID 140900

SEAN DEUBY (sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine*, and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

Windows IT Pro Congratulates NetWrix

NetWrix
#1 for Change Auditing and Compliance™

Community Choice Gold



Category: SharePoint
Product: NetWrix SharePoint Change Reporter

Editors' Best Bronze



Category: Auditing/ Compliance
Product: NetWrix Change Reporter Suite
Category: Management Suite
Product: NetWrix Enterprise Management Suite

Community Choice Silver



Category: Auditing/ Compliance
Product: NetWrix Change Reporter Suite
Category: Messaging
Product: NetWrix Exchange Change Reporter
Category: System Utility
Product: NetWrix Disk Space Monitor
Category: Systems Monitoring
Product: NetWrix Service Monitor

Community Choice Bronze



Category: Active Directory/ Group Policy
Product: NetWrix Change Reporter Suite
Category: Virtualization
Product: NetWrix VMware Change Reporter

Learn more about NetWrix here: www.netwrix.com • Phone #(888)638-9749(toll-free)

ADVERTISEMENT



Bagley

"Independently reviewed by industry experts these free tools proved to be useful for IT pros."



10 Holiday Gifts for IT Professionals

Audit Active Directory and file servers, securely manage passwords, detect inactive users and more – for free.

Here is the updated list of freeware tools by NetWrix Corporation which can save you a lot of time and make your network more efficient – at absolutely no cost. All of these tools also have advanced commercial editions with additional features, but the freeware editions will not expire, and will not stop working when you urgently need them.

1 **UPDATED! Active Directory Change Reporter** Active Directory Change Reporter (Windows IT Pro, Sep'09: InstantDoc ID 102446, TechRepublic: www.url2open.com/1v)— This simple auditing tool keeps tabs on what's going on inside your Active Directory. The Windows IT Pro 2010 Community Choice and Editors' Best Award-winner tracks changes to users, groups, OUs, and all other types of AD objects, sending detailed daily reports with lists of changes. **Download page**: www.url2open.com/1n

2 **NEW! Password Manager** (Active Directory Tools, Jun '11: www.url2open.com/1z) — A simple solution that gives the end users the ability to reset their forgotten passwords, troubleshoot account lockouts and unlock their accounts manually, through a secure web based interface, or a windows application that integrates with the Windows logon procedure. The new freeware version handles Google Apps, supports 10 languages and up to 50 users. **Download page:** www.url2open.com/1o

3 **Password Expiration Notifier** (Redmond Magazine Feb'09, 4sysops: www.url2open.com/1u) — This tool automatically reminds users to change their passwords before they expire, helping keep helpdesk administrators safe from password reset calls. It works nicely for users who don't log on interactively and, thus, never receive standard password change reminders at log on time (VPN and OWA). **Download page:** www.url2open.com/1m

4 **UPDATED! Privileged Account Manager** (SC Magazine: www.url2open.com/1q)—This product maintains a repository of privileged user accounts (such as Administrator, root, service accounts etc) in Active Directory, servers, and other systems, providing a secure web-based portal for role-based access and automatic maintenance of shared administrative user accounts. The tool can automatically generate strong passwords at specified intervals (e.g. every 30 days) and synchronize password changes on all target systems (for example, change service account password in Active Directory and update service credentials). **Download page:** www.url2open.com/1g

5 **Inactive Users Tracker** (MS TechNet Magazine May'08: www.url2open.com/1x, TechRepublic: www.url2open.com/1w) — This tool tracks down inactive user accounts (e.g., terminated employees) so you can easily disable them, or even remove them entirely, thus eliminating potential security holes. The tool sends reports on a regular schedule, showing what accounts have been inactive for a configurable period of time (e.g., 2 months). **Download page:** www.url2open.com/1l

6 **File Server Change Reporter** (4sysops.com: www.url2open.com/1t)—This is a must-have tool for auditing file servers and appliances. The tool detects changes made to files, folders and permissions, and tracks newly created and deleted files. The tool is useful for detecting mistakenly deleted files and it allows quick backup recovery of accidental changes. **Download page:** www.url2open.com/1k

7 **Active Directory Object Restore Wizard** (Windows IT Pro: www.url2open.com/1y) — This tool can save the day if someone accidentally (or intentionally) deletes important Active Directory objects. It provides granular object-level, and even attribute-level restore capabilities that allow quick rollbacks of unwanted changes (e.g., mistakenly deleted users, modified group memberships, etc). **Download page:** www.url2open.com/1j

8 **Windows Service Monitor** (WindowsReference.com: www.url2open.com/1r)—This very simple monitoring tool alerts you when some Windows service accidentally stops on one of your servers. The 2010 Windows IT Pro Community Choice and Editor's Best Award-winning tool also detects services that fail to start at boot time, which can happen, for example, with Microsoft Exchange. **Download page:** www.url2open.com/1h

9 **Disk Space Monitor** (MS TechNet Magazine Sep'09: www.url2open.com/1p)— Even with today's terabyte-large hard drives, server disk space tends to run out quickly and unexpectedly. This simple monitoring tool will send you daily reports regarding all servers that are running low on disk space, below the configurable threshold. **Download page:** www.url2open.com/1f

10 **VMware Change Reporter** (TechTarget/SearchVirtualDesktop: www.url2open.com/1s)—If you don't know what is being changed by your colleagues in the VMware infrastructure, it's very easy to get lost and miss changes that can affect things that you are responsible for. This 2010 Windows IT Pro Community Choice and Editor's Best Award-winner tracks and reports changes in VMware Virtual Center settings and permissions, such as newly created virtual machines, containers, alerts and more. **Download page:** www.url2open.com/1i

JOHN BAGLEY (john_bagley@sbcglobal.net) is an award-winning professional writer and independent consultant, who contributes to newspapers and magazines.

Scan this code with your Smartphone to get additional info

READER TO READER

Configuring Backup for DPM 2010

Every IT organization needs to perform backups because they ensure data integrity and recovery in the event of data loss caused by a system failure, accidental deletion by a user, or corruption. Yet backups are often treated as an afterthought. Sometimes the backup solution isn't architected properly or the systems providing the backups are underpowered. Other times the backup and restore procedures aren't well defined or routinely practiced until the unthinkable happens.



Anthony de Lagarde

One item that's regularly overlooked when architecting and implementing a backup solution is the use of a dedicated backup network that's separate from the production network, as Figure 1 shows. Each server to be backed up should have two network cards. The first network card should be used to connect to the production network; the second card should be used to connect to the backup network.

After I explain the benefits of using a dedicated backup network, I'll show you how to configure one for Microsoft System Center Data Protection Manager 2010. DPM 2010 provides disk- and tape-based backups for Microsoft OSs and line of business (LOB) applications that have Volume Shadow Copy Service (VSS) native support. Disk-based backups are intended for short-term data protection and rapid restores. Tape-based backups are intended for long-term data protection that's usually dictated by regulatory requirements. Disk- and tape-based backups can be combined to meet most organizations' backup and restore requirements. (For more information about DPM 2010, see technet.microsoft.com/en-us/systemcenter/dm/ff632007.)

The main benefit of using a dedicated backup network is that it separates the backup traffic from the traffic in the production environment, thereby avoiding the network congestion that can result when a large amount of data is backed up or restored. This congestion can slow the response times of applications, which can affect systems interoperability and user productivity.

An additional benefit of using a backup network is that you can use jumbo frames on a network card. This increases the Maximum Transmission Unit (MTU) size, which allows larger packets to be sent with less overhead from the underlying Ethernet media. Thus, the backup network can spend more time passing data and less time passing packet headers, which improves performance during backups and restores.

Not all network cards and switches support jumbo frames, so you need to check with your hardware provider to see whether your network cards and switches support this feature. In addition, if you plan to use Virtual LANs (VLANs) in the backup network, you must make sure your devices support using jumbo frames over a virtual interface.

To set up a backup network for DPM 2010, configure secondary network cards for the backup network, configure the HOSTS file on the DPM 2010 server, and specify the primary backup network. If your backup network will be providing system-state or bare-metal-recovery protection on a server running Windows Server 2008 or later, the Windows Server Backup Features must be installed on that server. Adding a feature to Server 2008 or later is outside the scope of this discussion; see the TechNet article "Adding Server Roles and Features" (technet.microsoft.com/en-us/library/cc732263.aspx) for guidance.

You first need to configure the secondary network cards for the backup network, making sure that they don't have any DNS entries, WINS entries, or default gateways.

1. Log on to one of the servers that will be backed up and rename its network cards to designate which network they're assigned to. In this example, they're renamed Backup and Production.
2. Right-click the Backup network card and select Properties. Click *Internet Protocol Version 4 (TCP/IPv4),* and select Properties.
3. Add the designated IP address and subnet mask, as Figure 2 shows. Don't assign a default gateway or any DNS servers.
4. Click the Advanced button, then select the DNS tab. Make sure no DNS

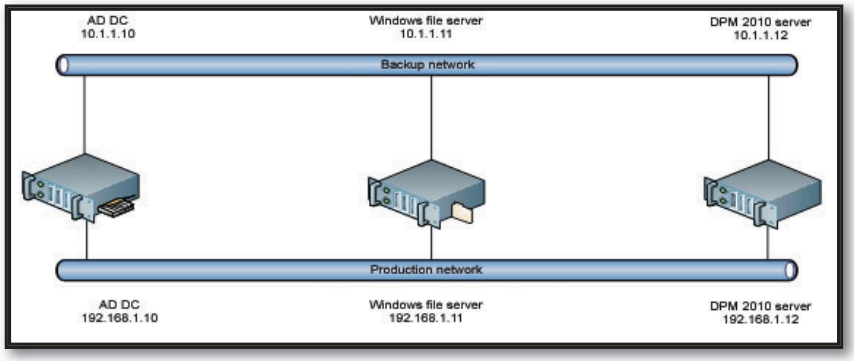


Figure 1: Architecting the dedicated backup network

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.
If we print your submission, you'll get $100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the Search box.

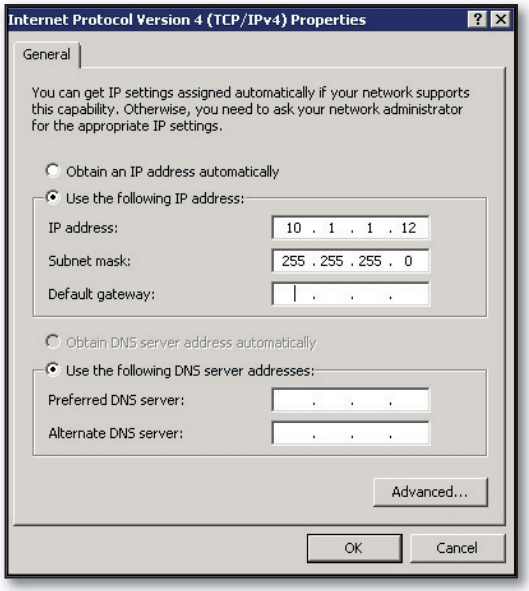


Figure 2: Configuring the IP address and subnet mask for a secondary network card

server entries are listed and the DNS suffix for the connection is blank.

5. Select the WINS tab and make sure no WINS servers are listed and NetBIOS over TCP/IP is enabled.
6. Click OK twice, then click Close.

You need to repeat steps 1 through 6 for the rest of the servers that will be backed up, including the DPM 2010 server. Take special precaution when configuring the Backup network card for the Active Directory (AD) domain controller (DC). There will be negative consequences to AD if its IP address is registered in DNS.

After you configure all the Backup network cards, open a command prompt on the DPM 2010 server and ping those cards' IP addresses to ensure there's connectivity. A common reason for not being able to connect is having a firewall blocking access.

It's now time to configure the DPM 2010 server's HOSTS file so that it contains all the IP addresses that have been assigned to the Backup network cards. On a Windows server, the HOSTS file is located in the C:\Windows\System32\drivers\etc folder. You need elevated administrative permissions to edit this file. Figure 3 gives an example of what the HOSTS file will look like after you add the IP addresses.

At this point, you can install the DPM agent on the servers to be backed up. Afterward, open the DPM Management Shell on the DPM 2010 server using the appropriate administrative privileges. (Your domain account must be part of the Local Administrators group.) The DPM Management Shell is built on top of Windows PowerShell.

Once opened, the DPM Management Shell's default folder is C:\Program Files\Microsoft Data Protection Manager\DPM\bin, as the last line in Figure 4 shows. After the command prompt, enter a command such as

```
Add-BackupNetworkAddress
  -Address 10.1.1.0/24
  -DPMServer MS-DPM-01
  -SequenceNumber 1
```

(Although this command wraps, you'd enter it all on one line.) This command uses the Add-BackupNetworkAddress cmdlet to tell DPM 2010 which network (in this case, 10.1.1.0/24) the DPM server (in this case, MS-DPM-01) should use as the primary backup network (indicated by -SequenceNumber 1).

You can specify a secondary network; for example, to instruct the DPM 2010 server to use the public network as a secondary backup network, use a command such as

```
Add-BackupNetworkAddress -Address
  192.168.1.0/24 -DPMServer MS-DPM-01
  -SequenceNumber 2
```

With the help of my colleague Jeff McMullen, I've demonstrated a general approach for deploying DPM 2010 on a dedicated backup network that most organizations can implement. By following this approach, you'll have a tool that will protect your data without clogging up your production network with traffic from backing up and restoring data.

—Anthony de Lagarde, senior infrastructure consultant, Microsoft Federal Practice

InstantDoc ID 140805

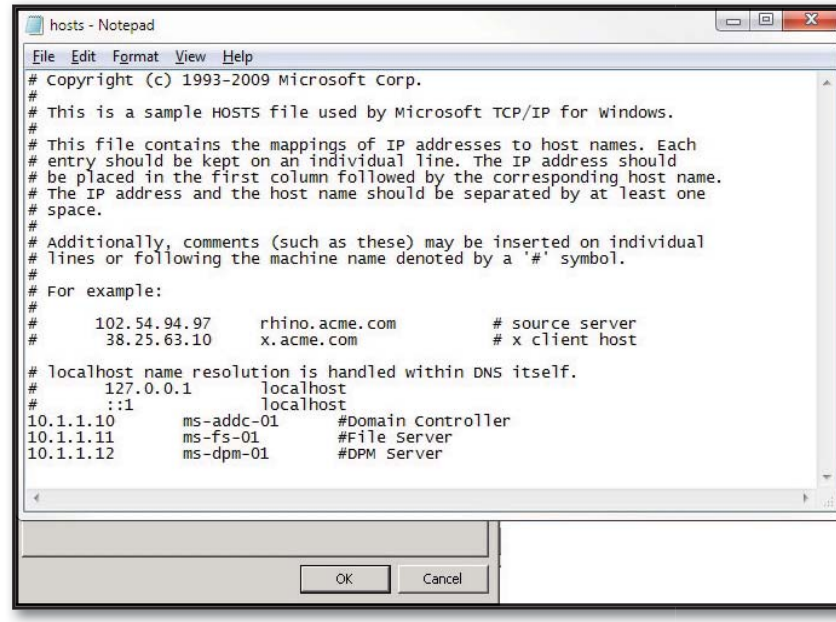


Figure 3: Configuring the HOSTS file



Figure 4: Using the DPM Management Shell to specify the primary backup network

Windows IT Pro Congratulates

HP



Windows IT Pro 2011 Editors' Best BRONZE

Category: **Hardware: Appliance**
Product: **HP E5000 Messaging System**
Award: **Editors' Best Bronze**

Learn more about the HP E5000 here: www.hp.com/go/e5000

Windows IT Pro Congratulates

HP



Windows IT Pro 2011
Editors' Best
GOLD

Category: **Messaging**
Product: **HP E5000 Messaging System**
Award: **Editors' Best Gold**

Learn more about the HP E5000 here: www.hp.com/go/e5000

- Windows 8
- VMware
- Security
- Hyper-V
- SID Roles
- SQL Server

ANSWERS TO YOUR QUESTIONS

Q: Will Windows 8 Server Hyper-V require the processor to support SLAT?

A: Installing Hyper-V on Windows 8 Client requires the processor to support Secondary Level Address Translation (SLAT). However, for Hyper-V on Windows 8 Server, SLAT is required only if the RemoteFX role service is enabled.

SLAT is a capability present in both Intel and AMD processors that allows the processor to handle the mapping of the physical memory to virtual memory for virtual machines (VMs) taking a workload from the processor. For Windows Server 2008 R2 SP1, SLAT is required on the server if the RemoteFX role service is enabled, because it's a huge benefit when dealing with graphically intensive operations.

For Windows 8 Client, most systems will be expected to have some high-end graphical capability (certainly compared to servers), and because of these higher-end graphics, SLAT is required on the processor if Hyper-V is to be used. For Windows 8 Server, SLAT isn't required unless the RemoteFX role service is enabled, in which case SLAT is required, as it is with Windows Server 2008 R2 SP1. Essentially, if your hardware runs Windows Server 2008 or Windows Server 2008 R2 Hyper-V, then it will run Windows Server 8 Hyper-V with the same features.

—John Savill

InstantDoc ID 140925

Q: Will Windows 8 client include Hyper-V?

A: Yes. In the MSDN blog post "Bringing Hyper-V to Windows 8" (blogs.msdn.com/b/b8/archive/2011/09/07/bringing-hyper-v-to-windows-8.aspx), Microsoft confirmed that the client version of Windows 8 will have Hyper-V support. That Hyper-V support includes the ability to access virtual machines (VMs) on file shares, support for touch via Remote Desktop Protocol (RDP) to the VMs, 32 vCPU and 512GB of RAM VMs, and Live Storage Move for a zero-downtime storage migration solution. Wireless networks will also be supported.

Additionally, unlike with Windows Server 2008 R2 Hyper-V systems today, the ability to sleep and hibernate a Windows 8 client with Hyper-V will be supported by descheduling the virtual CPUs from the VMs, which will effectively suspend them during a host sleep operation. Then, when the host is resumed, the virtual CPUs are rescheduled to the VM, which restarts the VMs.

—John Savill

InstantDoc ID 140678

Q: How do I put the Windows 8 ISO on a USB for USB installation?

A: For Windows 7, Microsoft's Windows 7 USB Download Tool could take an ISO file as input and write it out to a USB device, creating a bootable USB device containing the Windows 7 installation media.

This same application works for the Windows 8 Developer Preview ISOs as well. Download it from the Codeplex site (wudt.codeplex.com/releases/view/37074) or the Microsoft Store (www.microsoftstore.com/store/msstore/html/pbPage.Help—the link is near the bottom right; just search for Windows 7 USB/DVD Download Tool). Then pass the Windows 8 ISO as the input.

—John Savill

InstantDoc ID 140922

Q: My installation is stuck in "Pending file renames" and says it can't complete because these operations require a reboot—but after reboot, I still get the same error. How can I fix this?

A: Pending filename renames is a common operation needed by many setups to replace files that are currently in use and can't be replaced until a reboot.

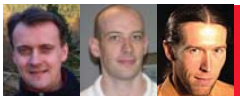
However, sometimes these operations get stuck and never complete. To fix, perform the following:

1. Start the registry editor (regedit.exe).
2. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager.
3. Double-click PendingFileRenameOperations.
4. Clear all the entries in the value and click OK.

The pending operations have now been removed and the installation you are performing should be able to finish.

—John Savill

InstantDoc ID 140680



Jan De Clercq | jan.declercq@hp.com
John Savill | jsavill@windowsitpro.com
Greg Shields | virtualgreg@concentratedtech.com

Q: How do I force a full shutdown of a Windows 8 machine including closing the kernel session information?

A: One of the reasons Windows 8 starts so fast normally is that it doesn't shut down the kernel session, which contains the system state and takes most of the time to start to initialize during system boot. Instead, the kernel session is actually hibernated, taking up a very small amount of disk space and making it quickly write and read again at startup.

This does mean that between boots, the system isn't re-initialized (because it's not typically needed). If you do make a hardware or system change that requires a system initialization, the system typically handles this for you automatically.

However, you can also force a full shutdown, and therefore full system initialization at next start, by adding the /full switch to the shutdown.exe command. For example, entering

```
shutdown /s /full /t 0
```

performs a full shutdown (not hibernating the kernel session) with no time delay. For more information on the boot changes in Windows 8, see the MSDN blog about boot times (blogs.msdn.com/b/b8/archive/2011/09/08/delivering-fast-boot-times-in-windows-8.aspx). It's a great read.

—John Savill

InstantDoc ID 140921

Q: How has performance improved for provisioning VMware vSphere 5.0 FDM agents?

A: When you enable vSphere 5.0's vSphere HA, the vCenter server provisions Fault Domain Manager (FDM) agents to each host in the cluster. The list of cluster hosts is also pushed to each FDM agent in parallel, enabling FDM agents to asynchronously engage in a master election. During this period, vCenter probes agents for the master, sending an alert if the election takes too long.

This parallel provisioning approach is different from the previous version's serial approach. It's expected to reduce cluster configuration time to less than one minute rather than the previous version's one minute per host.

—Greg Shields

InstantDoc ID 140942

Q: How are VMware vSphere's DRS Migration Threshold and *Target host load standard deviation* settings related?

A: vSphere Distributed Resource Scheduler (DRS) clusters have multiple configuration options that impact cluster behavior. One of those settings is the cluster's Automation Level, found under VMware DRS when viewing cluster properties. Three settings are available for Automation Level: Manual, Partially Automated, and Fully Automated.

When you select Fully Automated, a slider appears for setting the cluster's Migration Threshold. That threshold can be set between Conservative on the left and Aggressive on the right. Setting the slider to Conservative instructs the cluster to apply only priority 1 migration recommendations, and setting it to Aggressive instructs it to apply priority 1 through priority 5 recommendations. Selections between these two values apply recommendations scaling up from fewer on the Conservative end to more on the Aggressive end.

The Migration Threshold selection is directly related to the value for *Target host load standard deviation*, which is found under the cluster's Summary tab in the VMware DRS box. A more conservative Migration Threshold will drive a higher value for *Target host load standard deviation*, which will in turn define fewer VM migrations that an unbalanced cluster will apply to return that cluster to balance.

—Greg Shields

InstantDoc ID 140943

Q: What are the exact roles of a Windows account's SID, and more specifically its RID, for Windows security?

A: Every Windows user, computer, or service account has a unique alphanumeric identifier called the security ID (SID). Windows security-related processes, such as authentication, authorization, delegation, and auditing, use SIDs to uniquely identify security principals. Because SIDs are used by system processes, the format of a SID—unlike the format of a logon name—isn't user- or administrator-friendly.

To illustrate, let us analyze an example SID that I retrieved from my test Active Directory (AD) system: S-1-5-21-4064627337-2434140041-2375368561-1036. All SID fields have a specific meaning; so, for the above sample SID:

- S: The initial S identifies the following string as a SID.
- 1: The revision level, or version, of the SID specification. To date, this has never changed and has always been 1.
- 5: The identifier authority value. This is a predefined identifier for the top-level authority that issued the SID. This is typically 5, which represents the SECURITY_NT_AUTHORITY.
- 21-4064627337-2434140041-2375368561: This section is the domain or local computer identifier (in this example, a domain identifier). This is a 48-bit string that identifies the authority (the computer or domain) that created the SID.
- 1036: The Relative ID (RID) is the last part of a SID. The RID uniquely identifies a security principal relative to the local or domain security authority that issued the SID. Any group or user that the Windows OS doesn't create has a RID of 1000 or greater by default.

The SID of an AD domain account is created by a domain's security authority that runs on every Windows domain controller (DC). The SID of a local account is created by the Local Security Authority (LSA) service that runs on every Windows machine.

An important property of a SID is its uniqueness in time and place. A SID is unique in the environment where it was created (in a domain or on a local computer). It's also unique in time: If you create a user object, delete it, then re-create it with the same name, the new object won't have the same SID as the original object.

—Jan De Clercq

InstantDoc ID 141007

Q: Which log file contains vSphere HA information?

A: VMware vSphere 5.0 consolidates its status information for vSphere HA's Fault Domain Manager agent into a single log file. This behavior is unlike previous versions where multiple log files were used to store this information. The single log file, found at \var\log\fdm.log, provides information that can assist with issues related to partitioning, isolation, VM protection, agent election, and failover failures.

—Greg Shields

InstantDoc ID 140908

Q: The remote OS trying to connect to SQL Server Analysis Services is failing—what can I do?

A: This is most likely a firewall issue. First check that SQL Server Analysis Services is installed and running, which can be confirmed by running SQL Server Configuration Manager. Under SQL Server Services, you should see SQL Server Analysis Services and its state should be running, which Figure 1 shows.

If SQL Server Analysis Services is running, then you need to make sure the TCP firewall exception is enabled. This isn't automatically enabled by the SQL Server installation process. Here's how to check that it's enabled:

1. Start the Windows Firewall with Advanced Security application from the Administrative Tools folder.
2. Select Inbound Rules.
3. Select the New Rule action.
4. Select Port rule type and click Next.
5. Set the rule to type TCP, select the specific port, set it to 2383, and click Next.
6. Select *Allow the connection* and click Next.
7. Select the profiles to apply, such as Domain, and click Next.
8. Enter a name for the rule and click Finish.

—John Savill

InstantDoc ID 140682

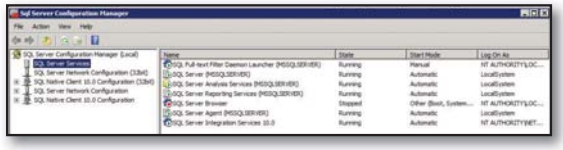


Figure 1: SQL Server Configuration Manager

Q: Is there a free solution to share my mouse between multiple computers and allow easy copying of data?

A: Microsoft offers Mouse Without Borders from its "Garage" program (blogs.technet.com/b/next/archive/2011/01/20/dirty-work-in-the-garage.aspx), which refers both to Building 4 at the Redmond campus (which has a cool layout fostering collaboration and creative thinking) and to Microsoft's fundamental premise of encouraging work on new solutions outside of employees' day jobs.

Mouse Without Borders is available at the TechNet blog (blogs.technet.com/b/next/archive/2011/09/09/microsoft-garage-download-mouse-without-borders.aspx). It lets up to four machines share a single mouse. You drag files between them and share a common clipboard by installing a small 1MB program.

Although it's called Mouse Without Borders, it also shares your keyboard and you can even lock all your machines at once with a simple keyboard shortcut, WindowsKey+L, as on a single machine.

The installation is simple, with no questions asked, and after installation, you are prompted if another machine has already been configured with Mouse Without Borders.

If this is the first machine, you click No, and a screen is displayed with a security code used to protect communication between machines and to stop someone from taking over your machine and your computer's name (see Figure 2). Keep this screen open or write down the security code.

Now install Mouse Without Borders on another machine, but this time, at the prompt, indicate that the software has already been installed on another machine.

You are then prompted to enter the security code and original computer's name. Enter this information, then click the LINK button. A progress screen is displayed, and you will be connected to your other machine. If a connection can't be made, you can try the IP address of the original machine, which you will need if the machines are in different domains (see Figure 3).



Figure 2: Mouse Without Borders security code



Figure 3: Mouse Without Borders machine setup

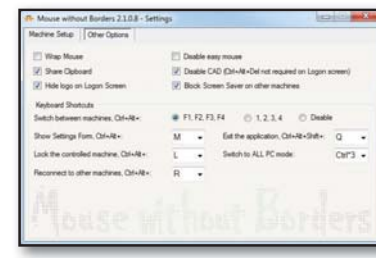


Figure 4: Mouse Without Borders settings

Once connected, a configuration screen is shown, letting you arrange the multiple computers and set options (see Figure 4). You can now use your keyboard and mouse across computers.

Note that each computer can have multiple displays: In my two-computer configuration, my main computer has three screens, and they all work just fine.

You can close the Mouse Without Borders dialog box, and the process stays running in the system tray, which allows access back to configuration and controlling the various machines. The machine where the mouse is currently active will respond to shortcut key combinations, such as WinKey+R to run an application.

—John Savill

InstantDoc ID 140907

2011 Windows IT Pro Editors' Best & Community Choice Awards

The polls have closed! Here are your—and our—favorite products of the year

by the *Windows IT Pro* editors

Most Encouraging IT Trends

1. Cloud computing
2. Virtualization
3. Increased security
4. Standardization
5. Social networking in the enterprise
6. Finding jobs
7. Reversing of previous offshoring decisions
8. Data deduplication
9. Tablets using the cloud
10. Free pancakes on Friday morning

Least Encouraging IT Trends

1. Cloud computing
2. Outsourcing
3. Mobile apps
4. Smaller budgets
5. Complexity of licensing
6. Storage costs
7. Proprietary solutions
8. Layoffs
9. Automation
10. Big players getting out of desktops/laptops

By providing two distinct perspectives on the market, the annual *Windows IT Pro* Editors' Best and Community Choice award programs offer a unique way to recognize the hottest products among the past year's offerings. Our Editors' Best program highlights products that *Windows IT Pro* editors and contributors believe are worthy of recognition, whereas our Community Choice program lets our readers decide which products are the best.

For the Community Choice program, we didn't just present a predefined list of products and services that limited your selection. Instead, we let you nominate your favorites, built the voting survey from there, and let everyone participate in the final voting phase. For our Editors' Best program, we also reached out to readers to find out how the Gold winners help you do your jobs. We spoke to real users about real experiences, and we hope these testimonials benefit you in your environment.

In these pages, you'll find our Gold, Silver, and Bronze Editors' Best winners directly adjacent to the Community Choice winners in each category. Sometimes our editors and readers agreed on favorite products and services in a given category, but more often they didn't. Choosing favorites from such a competitive field can be a challenge, but this year's winners show an uncommon breadth of functionality and originality.

Do you agree with our editors' choices? Or do our readers' picks carry more weight? Let us know! Regardless of whether the winners were chosen by editors or readers, you can be sure that all these products are worth serious consideration if you're in the market for a new tool.

Best Active Directory and Group Policy Product

Editors' Best

GOLD
Blackbird Auditor for Active Directory • Blackbird Group • www.blackbird-group.com

SILVER
ADManager Plus • Zoho • www.manageengine.com

BRONZE
GroupID • Imanami • www.imanami.com

Why It Won: Blackbird Auditor for Active Directory—a simple tool that integrates with Windows' native tools—offers real-time visibility into Active Directory (AD).

"Physician heal thyself" gains new meaning when it comes to diagnosing AD problems at a medical institution. In this case, ActiveSync devices were attacking the University of Mississippi Medical Center's AD via an ISA server, says senior systems administrator Josh Munn. "This process would have locked all mobile device users out of AD if we had a lockout policy in place," Munn explains. He'd done his research on all the major solutions and was testing another vendor's AD auditing product but found it complicated and time consuming. Then he discovered Blackbird Auditor for Active Directory. The product, Munn says, "was simple, affordable, and integrated with Windows native tools," and he downloaded and tested it with no issues: "Blackbird was able to help us [see] where the traffic was originating, thus giving a path in which to troubleshoot." Munn likes Blackbird because it lets him "see a baseline of AD traffic and determine whether it is daily, routine, or a possible attack. It also allows me to track what changes are being made to specialized groups within our AD environment. We really enjoy the real-time notifications that it sends if someone attempts to change an administrative group." Would he recommend it? Indeed—and one might say it's just what the IT doctor ordered.

Community Choice

GOLD
ActiveRoles Management Shell for Active Directory • Quest Software • www.quest.com

SILVER
ADManager Plus • Zoho • www.manageengine.com

BRONZE
Change Reporter Suite • NetWrix • www.netwrix.com

Other hot products in this year's survey . . .
Centrify Suite 2011
DameWare's NT Utilities
Quest Software's Active Administrator

"Put down your mouse—here comes Quest ActiveRoles! No other software has improved productivity and efficiency as much as this."

Best Auditing and Compliance Product

Editors' Best

GOLD
Centrify DirectAudit • Centrify • www.centrify.com

SILVER
VMware vCenter Configuration Manager • VMware • www.vmware.com

BRONZE
Change Reporter Suite •NetWrix • www.netwrix.com

Why It Won: DirectAudit 2.0 can easily replay a session, display the actual commands that were run in a list, and show both Windows and UNIX/Linux server sessions in one unified console.

"DirectAudit 2.0 has truly useful capabilities," said Sean Deuby, technical director for *Windows IT Pro*. "Replaying a session, in full-motion video, brings a new degree of insight to auditing sessions because it provides the auditor with an extra degree of context about what the user was doing during his session. Examining only the commands that were executed won't show the auditor what windows the user was opening, and what avenues he was exploring before he actually attempted to execute a command. Plus, Centrify's long track record of integrating UNIX and Linux into AD, and managing them holistically, only adds to its appeal."

Community Choice

GOLD
Centrify DirectAudit • Centrify • www.centrify.com

SILVER
Change Reporter Suite • NetWrix • www.netwrix.com

BRONZE
Control Compliance Suite • Symantec • www.symantec.com

Other hot products in this year's survey . . .
Quest Software's ChangeAuditor for Active Directory
Axceler's ControlPoint
NetIQ Secure Configuration Manager

Best Antivirus/Anti-Malware Product

Editors' Best

GOLD
Symantec Endpoint Protection • Symantec • www.symantec.com

SILVER
Endpoint Protection Suite • McAfee • www.mcafee.com

BRONZE
ESET NOD32 Antivirus 4 Business Edition • ESET • www.eset.com

Why It Won: Symantec has been a giant in the security industry for years, and it remains a dominant software provider for enterprise security solutions.

"Many *Windows IT Pro* readers dislike bloated, resource-sucking endpoint security products," says Jeff James, industry news analyst for *Windows IT Pro*, "and Symantec responded to the clamor for a more efficient and less resource-intensive security solution with Symantec Endpoint Protection 12 (SEP12). In addition to more efficient resource management, SEP12 leverages Insight (Symantec's cloud and community-based reputation technology) and SONAR, a program feature that Symantec claims is a hybrid behavioral-reputation engine that monitors applications, compares them with whitelisted apps, and checks for unusual behavior. For all of these reasons (and more), Symantec wins my vote as Best Antivirus/Anti-Malware product of 2011."

Community Choice

GOLD
Symantec Endpoint Protection • Symantec • www.symantec.com

SILVER
Comodo Internet Security 2011 • Comodo Group • www.comodo.com

BRONZE
ESET NOD32 Antivirus 4 Business Edition • ESET • www.eset.com

Other hot products in this year's survey . . .
Kaspersky's Anti-Virus for Windows Workstations
Malwarebytes' Anti-Malware
Trend Micro's OfficeScan

Best Backup Software Product

Editors' Best

GOLD
Replay • AppAssure Software • www.appassure.com
SILVER
Simpana • CommVault • www.commvault.com
BRONZE
Acronis Backup & Recovery • Acronis • www.acronis.com

Why It Won: AppAssure Software's Replay gives you top-tier backup, compression, deduplication, disaster recovery, and high-availability services in one box at a reasonable price.

Herb Thornton, network administrator at Brundage Bone, says, "My predecessor had a server fail at one of our remote locations. He had to purchase a new server, fly to that location and reinstall everything from scratch, then perform the file backup from tape. That branch didn't have access to its dispatching software for about five days; they had to do everything on paper during that time! A month after I purchased AppAssure, I ran into the same scenario. A server quit and refused to start at one of my remote locations, and nobody was able to diagnose the reason. I was able to take the latest snapshot and fire up a virtualized image of the server. I had the employees remote into their virtualized server and had them back up and dispatching within 20 minutes. I then concentrated on doing a bare-metal restore on another server. I was able to get the server restored to a different unit, test it, and get it shipped to the location by the next day. They simply plugged the replacement server in at their location, I pushed the updated changes back to the replacement server from the virtualized server, and it was business as usual. AppAssure paid for itself that day."

Community Choice

GOLD
Symantec NetBackup • Symantec • www.symantec.com
SILVER
Acronis Backup & Recovery • Acronis • www.acronis.com
BRONZE
Veeam Backup & Replication • Veeam Software • www.veeam.com

Other hot products in this year's survey . . .
AppAssure's Replay
NetApp Syncsort Integrated Backup (NSB)
Acronis True Image

Best Cloud Computing Product or Service



Editors' Best

GOLD
Dropbox • Dropbox • www.dropbox.com
SILVER
Google Apps • Google • www.google.com
BRONZE
Rackspace • Rackspace • www.rackspace.com

Why It Won: Dropbox epitomizes why the cloud computing revolution is so compelling.

"Dropbox is so useful that even IT pros and their managers (who won't formally support Dropbox) use it themselves," says Sean Deuby, technical director for *Windows IT Pro*. "At a recent IT security conference, a speaker asked the audience how many supported Dropbox. Only a few raised their hands. When asked how many used it themselves, about 60 percent raised their hands. The Dropbox (Software as a Service—SaaS) application and local clients provide a simple yet powerful method, using cloud storage, to share and synchronize files between PCs, tablets, and smartphones. You can share Dropbox folders with others for simple, ad-hoc collaboration that's easier to use than Microsoft SharePoint. And the tablet and mobile app community have embraced Dropbox to integrate it into many popular mobile apps such as QuickOffice."

Community Choice

GOLD
VMware vCloud Director • VMware • www.vmware.com
SILVER
Dropbox • Dropbox • www.dropbox.com
BRONZE
Google Apps • Google • www.google.com

Other hot products in this year's survey . . .
Amazon Elastic Compute Cloud (EC2)
Symantec.cloud
Smith Micro Software's SendStuffNow

"VMware vCloud Director really eases the migration to cloud."

Best Deployment/ Configuration Product

Editors' Best

GOLD
Desktop Authority • ScriptLogic • www.scriptlogic.com
SILVER
DocAve Deployment Manager • AvePoint • www.avepoint.com
BRONZE
VMware vCenter Configuration Manager • VMware • www.vmware.com

Why It Won: Desktop Authority is a full-featured deployment, configuration, and management product that reduces complicated tasks to simple point-and-click processes.

As the IT director for the college of architecture, design, and construction at Auburn University, Scott Davis must manage numerous output devices for the students and faculty. Because of the nature of these programs, Davis says, "printing here is paramount, and that was really a driving factor to look at ScriptLogic when I did." He had been managing permissions through Visual Basic (VB) scripts, but with the frequent changes of students, classrooms, and levels of permissions, "it was turning into a hydra, it was just incredibly complex." Upon implementing Desktop Authority, Davis "was able to get rid of all those [VB] scripts. I was able to map all the drives, everything, probably within 10 minutes. It literally took a day's worth of work and crunched it down to 15 minutes while I drank my coffee. Of course, we haven't looked back."

Community Choice

GOLD
VMware vCenter Configuration Manager • VMware • www.vmware.com
SILVER
Desktop Central • Zoho • www.manageengine.com
BRONZE
Altiris Deployment Solution • Symantec • www.symantec.com

Other hot products in this year's survey . . .
Symantec's Norton Ghost
Dell's KACE K2000 Deployment Appliance
AvePoint's DocAve Deployment Manager

"VMware vCenter Configuration Manager is an awesome product, one of the best for virtualization management—highly recommended!"

Best Hardware: Server

Editors' Best

GOLD
HP ProLiant DL580 G7 • HP • www.hp.com

SILVER
PowerEdge R910 • Dell • www.dell.com

BRONZE
ThinkServer RD240 • Lenovo • www.lenovo.com

Why It Won: The HP ProLiant DL380 G7 is a terrific high-performance virtualized server, ideal for building the private cloud.

"One of the most important growing trends in IT is the private cloud," says Michael Otey, technical director for *Windows IT Pro*, "and one of the core components that goes into building the private cloud is high-performance virtualized servers. The HP DL580 G7 is a 4U rack-mounted server with four sockets supporting Intel Xeon 7500 processors with up to 10 cores, giving it the computing power necessary to handle enterprise-class workloads. Memory can be a limiting factor in the number of virtual machines (VMs) that can run concurrently, and the HP DL580 supports up to 2TB of RAM, making it a highly scalable virtualization platform. HP's Systems Insight Manager and Integrated Lights-Out (iLO) management technology provide robust out-of-band server management capabilities."

Community Choice

GOLD
PowerEdge • Dell • www.dell.com

SILVER
HP ProLiant • HP • www.hp.com

BRONZE (tie)
Cisco Unified Computing System • Cisco • www.cisco.com
IBM BladeCenter • IBM • www.ibm.com

Other hot products in this year's survey . . .
HP BladeSystem
Stratus's ftServer
Lenovo's ThinkServer



Best Hardware: Workstation

Editors' Best

GOLD
Dell Precision T7500 • Dell • www.dell.com

SILVER:
ThinkStation C20 • Lenovo • www.lenovo.com

BRONZE:
HP Pavilion HPE h8m • HP • www.hp.com

Why It Won: Dell Precision workstations give you a personal supercomputer.

"Today's high-performance desktops offer much more processing power than the servers of just a couple of years ago," says Michael Otey, technical director for *Windows IT Pro*. "With support for dual six-core Xeon X5690 processors and up to 192GB of RAM, the Dell Precision T7500 provides all the power you might want for running multiple development VMs, running resource-intensive graphical rendering programs, or just providing a super-fast application development and testing platform. Dell calls this system 'your own personal supercomputer' because you can optionally have it delivered with the 448 CUDA core NVIDIA Tesla video card. CUDA is an advanced parallel processing architecture, and CUDA-enabled applications can harness the power in the GPU for extreme processing performance."

Community Choice

GOLD
Dell OptiPlex • Dell • www.dell.com

SILVER
Mac Pro • Apple • www.apple.com

BRONZE
HP Compaq • HP • www.hp.com

Other hot products in this year's survey . . .
Dell's Precision
Lenovo's ThinkCenter

"We don't often keep a desktop system for 10 years, but when we do, it's an OptiPlex!"

Best Hardware: Laptop

Editors' Best

GOLD
ThinkPad T420s • Lenovo • www.lenovo.com

SILVER
HP ProBook 5330m • HP • www.hp.com

BRONZE
MacBook Pro • Apple • www.apple.com

Why It Won: An impressive combination of specs, design, durability, and competitive pricing make the Lenovo ThinkPad T420s hard to beat.

"The average Windows business laptop has been characterized as being dull and uninspired compared with flashier offerings from Apple and Sony," says Jeff James, industry news analyst for *Windows IT Pro*, "but that trend is starting to change. Helping lead the charge is Lenovo, which has been introducing business laptops that manage to combine impressive features with quality, performance, and aggressive pricing. One of the best of this breed is the Lenovo ThinkPad T420s, which weighs in at four pounds with a 14-inch screen and a robust spec sheet, including USB 3.0 and an Intel dual-core i5 CPU. It's a bit pricier than more value-oriented notebooks, but you often get what you pay for."

Community Choice

GOLD
Dell Latitude • Dell • www.dell.com

SILVER
ThinkPad • Lenovo • www.lenovo.com

BRONZE
MacBook Pro • Apple • www.apple.com

Other hot products in this year's survey . . .
HP's EliteBook
Toshiba's Satellite
Dell's Alienware

"The Latitude works . . . and works . . . and works. We've had no problems, and support is amazing, even sharing tips and tricks to boost productivity."

Best Hardware: Networking



Editors' Best

GOLD
BIG-IP product family • F5 Networks • www.f5.com

SILVER
Barracuda Load Balancer • Barracuda Networks • www.barracudanetworks.com

BRONZE
AX 3000-11 • A10 Networks • www.a10networks.com

Why It Won: F5 Networks' BIG-IP product family offers impressive load-balancing and application-delivery functionality. It's a versatile, easy-to-deploy, high-performance juggernaut.

"We migrated to the F5 BIG-IP from a competitor's solution that wasn't meeting our needs," says Brad Trankina, director of network and information systems at Human Kinetics. "After reviewing several alternatives, we selected BIG-IP because we thought it was the best product on the market. We have been extremely impressed with the performance, stability, and reliability of this enterprise-class product. While the BIG-IP has been a huge improvement over our previous solution, we have been most impressed by the support provided by F5 [Networks]. From implementation through the few occasions we've contacted support, the company has gone above and beyond our expectations. This includes assisting us with issues with our websites after it was determined the problem was not being caused by the BIG-IP."

Community Choice

GOLD
Cisco Catalyst 6500 Series • Cisco Systems • www.cisco.com

SILVER
HP Networking • HP • www.hp.com

BRONZE
Juniper Networks SRX Series • Juniper Networks • www.juniper.net

Other hot products in this year's survey . . .
F5 Networks' BIG-IP Local Traffic Manager
Cisco Nexus 5000
Barracuda Networks' Barracuda Load Balancer

Best Hardware: Storage

Editors' Best

GOLD
Hyper ISE • XIO Storage • www.xiostorage.com

SILVER
B1200i • Drobo • www.drobo.com

BRONZE
StorSimple 7010 • StorSimple • www.storsimple.com

Why It Won: At a turning point in the trajectory of the storage industry, XIO—with its awesome Hyper ISE—is pioneering a unique path that focuses on performance rather than capacity.

"Microsoft Partner Solutions Center (MPSC) hardware-testing projects are designed to put maximum stress on systems so that customers can have the utmost confidence in deploying them in support of business-critical functions," says David Hayes, director of the MPSC. "In such a demanding context, XIO Hyper ISE performed beyond our wildest expectations with the HDD/SSD solution that we tested. Where most storage systems have underperformed before, we felt like we hardly put a dent in the Hyper ISE performance potential. We estimate it would take an increase of workload by a factor of 10 to push the Hyper ISE we tested to its actual performance threshold. We're looking forward to deploying it in the MPSC environment."



Community Choice

GOLD
NetApp FAS6200 Series • NetApp • www.netapp.com

SILVER
EMC VNX • EMC • www.emc.com

BRONZE
Dell EqualLogic • Dell • www.dell.com

Other hot products in this year's survey . . .
Dell's PowerVault
EMC's Symmetrix VMAX
HP's Enterprise Virtual Array (EVA)

Best Hardware: Appliance

EMC²

Editors' Best

GOLD
EMC Greenplum Modular Data Computing Appliance (DCA) • EMC • www.emc.com

SILVER
Dell Kace M300 Asset Management Appliance • Dell • www.kace.com

BRONZE
HP E5000 Messaging Systems • HP • www.hp.com

Why It Won: As data sizes continue to grow exponentially, big data analytics is a booming field with lots of growth potential, and EMC—with its Greenplum Modular DCA—is helping to lead the way.

"Midsized-to-large enterprises must deal with rapidly expanding data storage needs as well as pressing business demands to quickly analyze and process vast amounts of structured and unstructured data," says Jeff James, industry news analyst for *Windows IT Pro*. "Big data analytics is a fast-growing industry, and perhaps no other company is making as big a push as EMC with its Greenplum Modular DCA. Leveraging massively parallel processing (MPP) and Apache Hadoop, the Greenplum DCA helps larger organizations derive value out of their massive stockpiles of customer and corporate data."

Community Choice

GOLD
Barracuda Spam & Virus Firewall • Barracuda Networks • www.barracudanetworks.com

SILVER
Dell KACE K1000 Management Appliance • Dell • www.dell.com

BRONZE
NetBackup 5000 Series • Symantec • www.symantec.com

Other hot products in this year's survey . . .
SonicWALL's NSA Series
HP's Business Decision Appliance
Riverbed Technology's Steelhead product family

Most Overused IT Buzzwords

1. Cloud
2. Cloud
3. Cloud
4. Cloud
5. Cloud
6. Cloud
7. Cloud
8. Virtual
9. Social networking
10. Tablet

Windows IT Pro Magazine Congratulates **VMware**

Windows IT Pro magazine

vmware®



Editors' Best Awards

Category: **Virtualization**
Product: **VMware vSphere 5**
Award: **Editors' Best Gold**



Editors' Best Silver

Category: **Auditing/ Compliance**
Product: **VMware vCenter Configuration Manager**
Award: **Best Silver**



Editors' Best Bronze

Category: **Deployment/ Configuration**
Product: **VMware vCenter Configuration Manager**
Award: **Editors' Best Bronze**



Community Choice Gold

Category: **Cloud Computing**
Product: **VMware vCloud Director**

Category: **Deployment/ Configuration**
Product: **VMware vCenter Configuration Manager**



Community Choice Silver

Category: **High Availability/ Disaster Recovery**
Product: **VMware vCenter Site Recovery Manager**

Category: **Virtualization**
Product: **VMware vSphere**

Learn more about VMware here: www.vmware.com • 877 - 486 - 9273

vmware



Cloud can be confusing. Your cloud doesn't have to be.

When it comes to cloud computing, everyone seems to have a different point-of-view. It can be pretty overwhelming. As the global leader in virtualization and cloud infrastructure, VMware would like to help. We're here to cover the important topics, provide the latest research and answer all your questions. And when you're ready, we'll help you build the perfect cloud solution, one that leverages your existing IT resources and aligns seamlessly with the specific needs of your enterprise. So, ask away and let's get started with your cloud.

Get your questions answered at **http://www.vmware.com/go/yourcloud/nam**

© 2011 VMware, Inc. All rights reserved.

Best High-Availability/Disaster-Recovery Product



Editors' Best

GOLD
Replay • AppAssure Software • www.appassure.com

SILVER
Veritas Storage Foundation HA for Windows • Symantec • www.symantec.com

BRONZE
CA ARCserve High Availability • CA • www.arcserve.com

Why It Won: Replay provides high availability, disaster recovery, backup, deduplication, and compression services in one box at a reasonable price.

"With the cost of tape getting higher, we couldn't back up everything we wanted," says Scott Poole, network manager at Linkage. "With AppAssure, I bought four very inexpensive mini SANs and used one in Massachusetts and one in Georgia, and I'm doing backup of up to 4TB with AppAssure's compression, and already getting 10 times more data than before. I'm using only 2TB even though we can now back up all the non-critical data as well. Not only that, we now have a disaster-recovery plan in place with our office in Atlanta, where I replicate data throughout the day. We're using AppAssure in virtual standby for Exchange Server and SQL Server systems for seamless disaster recovery. AppAssure has come through with flying colors and frankly has made me look like a rock star."

Community Choice

GOLD
Veritas Storage Foundation HA for Windows • Symantec • www.symantec.com

SILVER
VMware vCenter Site Recovery Manager • VMware • www.vmware.com

BRONZE
Veeam Backup & Replication • Veeam Software • www.veeam.com

Other hot products in this year's survey . . .
AppAssure's Replay
Commvault's Simpana
FalconStor's Continuous Data Protection (CDP)

Best Interoperability Product

Editors' Best

GOLD
MapForce • Altova • www.altova.com

SILVER
NETsec GALsync • NETsec • www.netsec.de

BRONZE
Skytap Cloud • Skytap • www.skytap.com

Why It Won: Altova MapForce provides a no-code way to integrate data from multiple, diverse sources through a drag-and-drop interface.

"With data accumulating at increasing rates, from different sources and in different formats, having the ability to pull it all together into one useful report is a must," said B. K. Winstead, senior associate editor for *Windows IT Pro*. "That's why Altova MapForce is the winner of Editors' Best in the Interoperability category this year. With the drag-and-drop graphical interface, you can create simple one-to-one data mappings—for example, from a Microsoft SQL Server database to an XML file—or more complex mappings with multiple data sources or split to multiple targets and involving various filters from the built-in library, or with your own functions created through the visual function builder. MapForce works with many data types and can output into a variety of code formats for easy implementation—a true 'no code' solution to data integration and mapping."

Community Choice

GOLD
RealVNC • RealVNC • www.realvnc.com

SILVER
Centrify DirectControl • Centrify • www.centrify.com

BRONZE
NTFS for Mac OS X • Paragon Software Group • www.paragon-software.com

Other hot products in this year's survey . . .
Skytap Cloud
NETsec's GALsync
Altova's MapForce

"Nothing else really comes close to RealVNC."

Best Management Suite

Editors' Best

GOLD
Quest One Identity Manager • Quest Software • www.quest.com

SILVER
Spiceworks MyWay • Spiceworks • www.spiceworks.com

BRONZE
Enterprise Management Suite • NetWrix • www.netwrix.com

Why It Won: Quest One Identity Manager is a management suite for that most important component of your IT infrastructure: the digital identities of your users.

"In my experience, most companies have some degree of difficulty managing the life cycle of provisioning, changing, and de-provisioning a user's identity," says Sean Deuby, technical director for *Windows IT Pro*. "And it's not just the management of a user's account in a central repository such as AD; an identity management system must seamlessly handle identities across multiple stores that might not otherwise share data with each other. Even though many are looking to the cloud for their future, to be successful there you must get your identity infrastructure in order first. Quest has been actively building out its portfolio of identity and access management (IAM) products, and the acquisition of Voelcker Informatik's ActiveEntry product (now Quest One Identity Manager) brings strong life-cycle management capabilities to its One Identity Solution IAM suite. I especially like One Identity Manager's ability to give users some degree of self-service to control accounts and access rights and permissions without admin intervention."

Community Choice

GOLD
Spiceworks MyWay • Spiceworks • www.spiceworks.com

SILVER
Altiris IT Management Suite • Symantec • www.symantec.com

BRONZE
Veeam ONE • Veeam Software • www.veeam.com

Other hot products in this year's survey . . .
NetWrix's Enterprise Management Suite
HP Insight Management
SolarWinds' Orion

Favorite IT Websites

1. www.google.com
2. www.experts-exchange.com
3. www.spiceworks.com
4. www.microsoft.com
5. www.winsupersite.com
6. www.windowsitpro.com
7. www.theregister.co.uk
8. www.techtarget.com
9. www.networkworld.com
10. www.engadget.com

Best Microsoft Product



Editors' Best

GOLD
OneNote 2010 • Microsoft • www.microsoft.com

SILVER
Windows 7 • Microsoft • www.microsoft.com

BRONZE
Hyper-V Server 2008 R2 • Microsoft • www.microsoft.com

Why It Won: Microsoft OneNote, especially its 2010 incarnation, is one of the most underappreciated Microsoft products available today.

"This was a hard choice," says Sean Deuby, technical director for *Windows IT Pro*. "I really love Windows 7 and the way it's improved the desktop experience. However, I use OneNote 2010 as the repository for pretty much any useful information I might ever want to look at again, both professionally and personally: task lists, product information (such as 10-plus years of AD tidbits), meeting notes, projects . . . it's all in there. In addition to its terrific outlining capabilities, OneNote lets you take screenshots, record audio or video that synchronizes with the notes you're taking, perform real-time collaboration, and publish meeting minutes instantly. I synchronize my three OneNote 2010 notebooks across multiple systems using Windows Live SkyDrive, and it all simply works."

Community Choice

GOLD
Windows 7 Professional • Microsoft • www.microsoft.com

SILVER
Exchange Server 2010 • Microsoft • www.microsoft.com

BRONZE
Windows Server 2008 R2 • Microsoft • www.microsoft.com

Other hot products in this year's survey . . .
Microsoft Office 2010
Microsoft SharePoint 2010
Microsoft SQL Server 2008 R2

"Windows 7 Professional is perhaps Microsoft's best OS—simple, efficient, intuitive, user-friendly, productive."

Favorite Consumer Tech Products

1. Apple iPad
2. Apple iPhone
3. Windows Phone
4. Microsoft Xbox 360
5. HTC smartphones
6. Barnes & Noble Nook Color
7. Samsung Galaxy
8. Asus EEE Transformer
9. Canon Pixma printers
10. RIM BlackBerry Torch

Most Overhyped Consumer Tech Products

1. Apple anything
2. Apple iPad
3. Apple iPhone
4. RIM BlackBerry devices
5. Android anything
6. e-Readers
7. Tablets
8. Microsoft Office
9. Online speed-booster programs
10. Microsoft Xbox 360

Best Messaging Product

Editors' Best

GOLD
HP E5000 Messaging System • HP • www.hp.com

SILVER
Transend Migrator • Transend • www.transend.com

BRONZE
Mailscape • ENow • www.enowconsulting.com

Why It Won: HP, in partnership with Microsoft, did what was once said couldn't be done: They put an entire Exchange Server environment in a box.

"So much of the talk these days is about Microsoft Offic 365 and the cloud, but not all organizations—large or small—consider the cloud or hosted model to be acceptable to their needs, even while the benefits of a full-featured Microsoft Exchange Server deployment might be too costly or complex to implement," says B. K. Winstead, senior associate editor for *Windows IT Pro*. "That's why the HP E5000 Messaging System appliance is this year's Editors' Best pick. You get all the benefits of an Exchange 2010 organization in a preconfigured appliance, including the Windows OS, high availability with database availability groups (DAGs), and storage on Direct Attached Storage (DAS). You can choose to have mailboxes with either 1GB or 2.5GB quotas. With the wizard-based set-up tools, you can be up and running with your Exchange environment in a matter of hours. This one is well worth looking into!"

Community Choice

GOLD
Skype for Business • Skype • www.skype.com

SILVER
Exchange Change Reporter • NetWrix • www.netwrix.com

BRONZE
IBM Lotus Domino • IBM • www.ibm.com

Other hot products in this year's survey . . .
ENow's Mailscape
Transend Migrator
GFI Software's GFI MAX MailProtection

"Everyone loves Skype! Easy-to-use chat, voice, and video! Microsoft, please don't screw it up!"

Best Mobile and Wireless Product

Editors' Best

GOLD
Windows Phone 7.5 • Microsoft • www.microsoft.com
SILVER
Zenprise MobileManager • Zenprise • www.zenprise.com
BRONZE
Apple iOS • Apple • www.apple.com

Why It Won: Windows Phone 7 was already the superior smartphone platform, but Windows Phone 7.5 is even better.

"Conceptually, [Windows Phone] 7.5 isn't hugely different from its predecessor," said Paul Thurrott, senior technical analyst for *Windows IT Pro*. "See, Microsoft got the basics right with Windows Phone 7. The foundation is solid. So this time around, it was all about filling in the missing features. This is evolution at its finest. In many ways, Windows Phone 7.5 is to Windows Phone 7 as Windows 7 was to [Windows] Vista: the same basic OS, but streamlined, spit-shined, and made better. There are a few big changes, but most of the many new features in this release are small tweaks to existing features. But these little changes really add up. They're everywhere." Windows Phone 7.5 is a free upgrade for all existing Windows Phone 7 handsets.

Community Choice

GOLD
Apple iOS • Apple • www.apple.com
SILVER
Google Android • Google • www.google.com
BRONZE
Windows Phone • Microsoft • www.microsoft.com

Other hot products in this year's survey . . .
Research In Motion's BlackBerry Professional Software
Rockliffe's AstraSync
Skype

"You mean there's still competition out there for Apple? How can that be? It's the most flexible, feature-rich, adaptable, cost-effective solution."

Best Patch-Management Product

Editors' Best

GOLD
VMware vCenter Protect Essentials Plus • VMware • www.vmware.com
SILVER
Desktop Central 7 • Zoho • www.manageengine.com
BRONZE
GFI LanGuard 2011 • GFI Software • www.gfi.com

Why It Won: Patch management can be an ugly, thankless task, but VMware vCenter Protect Essentials Plus (formerly Shavlik NetChk Protect) makes it a snap.

"Patch management is one of the most onerous tasks that any IT pro has to deal with," says Jeff James, industry news analyst for *Windows IT Pro*, "and a good patch-management application can make a huge difference. Several patch-management programs are available on the market, but only a few offer the number of features that today's IT pros demand. Shavlik has been a leader in the patch-management space for years, and several other patch-management vendors license Shavlik technology for their own products. Shavlik was acquired by VMware in May 2011, and VMware has made it clear that it intends to enhance the Shavlik patch-management product portfolio even further by leveraging VMware's strengths in virtualization and cloud computing."

Community Choice

GOLD
Altiris Client Management Suite • Symantec • www.symantec.com
SILVER
VMware (Shavlik) Patch Management • VMware • www.vmware.com
BRONZE
GFI LanGuard • GFI Software • www.gfi.com

Other hot products in this year's survey . . .
NetIQ Secure Configuration Manager
ScriptLogic's Desktop Authority

"Altiris has reduced our TCO for all systems; we're managing and troubleshooting our network from anywhere. Good stuff!"

Best Network-Management Product

Editors' Best

GOLD
Orion Network Performance Monitor • SolarWinds • www.solarwinds.com
SILVER
Foglight • Quest Software • www.quest.com
BRONZE
EventSentry • netikus • www.netikus.net

Why It Won: Orion Network Performance Monitor offers excellent enterprise-class network-management capabilities at a reasonable price.

SolarWinds' network-management tools have a fan base that just seems to keep coming back for more. "Orion Network Performance Monitor is the Swiss Army knife of monitoring solutions," said John Spanitz, senior systems administrator at Just Born. "Through its unified views, we get a clear picture of what's going on across all aspects of our environment—without having to use a bunch of different tools." Orion's modular design lets you pick and choose exactly what you need for your business. The product's network maps are particularly noteworthy, allowing you to pinpoint where problems are occurring in the environment. SolarWinds' support team is almost legendarily responsive, and the company's Thwack community leads the way in vendor/customer interaction.

Community Choice

GOLD
Orion Network Performance Monitor • SolarWinds • www.solarwinds.com
SILVER
LogMeIn Central • LogMeIn • www.logmein.com
BRONZE
Citrix NetScaler • Citrix • www.citrix.com

Other hot products in this year's survey . . .
Spiceworks MyWay
Paessler's PRTG Network Monitor
Ipswitch's WhatsUp Gold

"SolarWinds provides a powerful monitoring solution with all features included, and yet it's really easy to use. And I love the look and feel."

Reliability for your growing business. Expertise you can depend on.

The IBM System x3650 M3 Express® server with the latest Intel® Xeon® processor 5600 series offers you the reliability to run business-critical workloads. Its comprehensive system management tools constantly monitor the health of the system and help you easily diagnose an impending issue. The reliable x3650 M3, with the valuable expertise of IBM Business Partners, can help you to confidently run your business.

Rated No. 1 in Server Customer Satisfaction by TBR for the 8th consecutive quarter.[1]



IBM System x3650 M3 Express

$2,799

OR $80/MONTH FOR 36 MONTHS[2]

PN: 7945-E6U

- Improve cost-effectiveness with higher performance per watt
- Simplify management and serviceability with flexible design
- Manage risk with resilient architecture



IBM System x3400 M3 Express

$1,699

OR $49/MONTH FOR 36 MONTHS[2]

PN: 7379-E5U

- Optimum performance and processing capability at a low cost
- Large storage capacity and flexible configurations to scale as needs grow
- Reduced energy costs and simple management

IBM System Storage® EXP2500 Express



$3,399

OR $97/MONTH FOR 36 MONTHS[2]

PN: 174712X

- Designed for IBM System x direct attachment via ServeRAID M5025 adapter
- High capacity, with support for multiple enclosures per configuration
- High availability and reliability, with dual AC power supplies and fans

IBM Systems Consolidation Evaluation Tool

See how much you can save on your IT costs.
Log on at **ibm.com/systems/reliability**

Scan with your smart phone to learn more about the x3650 M3

Contact the IBM Concierge to help you connect to the right IBM Business Partner.

1 866-872-3902 (mention 601BB01A)

or Search x3650m3

[1]TBR 2Q11 x86-Based Servers: Corporate IT Buying Behavior & Customer Satisfaction Study, August 2011.
[2]Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. IBM hardware products are manufactured from new parts or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit http://www.ibm.com/servers/support/machine_warranties. IBM makes no representation or warranty regarding third-party products or services. IBM, the IBM logo, Express, System Storage and System x are registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. For a current list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. All prices and savings estimates are subject to change without notice, may vary according to configuration, are based upon IBM's estimated retail selling prices as of 9/22/11 and may not include storage, hard drive, operating system or other features. Reseller prices and savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area. ©2011 IBM Corporation. All rights reserved.

intel Xeon inside™

Powerful. Intelligent.

Best Scripting Tool

Editors' Best

GOLD
Idera PowerShell Plus • BBS Technologies • www.idera.com
SILVER
PowerWF Studio • Devfarm Software • www.powerwf.com
BRONZE
PrimalScript • SAPIEN Technologies • www.sapien.com

Why it Won: PowerShell is quickly becoming one of the most important tools available for systems administrators, and Idera PowerShell Plus makes it easier to learn and use.

"Initially released in 2006, PowerShell has evolved over the years to become an extremely powerful tool for Windows systems administrators," says Jeff James, industry news analyst for *Windows IT Pro*. "But not everyone is keen on spending much time banging out code from the command line, and that's where one of the many PowerShell integrated development environments (IDEs) come into play. There are several options on the market, but Idera PowerShell Plus is one of the best. Idera purchased Tobias Weltner's PowerShellPlus several years ago, and Idera has begun to finally update the product on a more aggressive schedule. Version 4.0 introduced a revamped UI and enhanced script debugging, and 4.1 introduces version control using MSCCI-compliant plug-ins and new scriptable APIs to automate the PowerShell Plus IDE."

Community Choice

GOLD
PowerGUI Pro • Quest Software • www.quest.com
SILVER
Idera PowerShell Plus • BBS Technologies • www.idera.com
BRONZE
PrimalScript • SAPIEN Technologies • www.sapien.com

Other hot products in this year's survey . . .
Specops Software's Specops Command
FastTrack Software's FastTrack Scripting Host

"Wow! PowerGUI is so powerful, I was really shocked by how much time it saves me!"

Best SharePoint Product

Editors' Best

GOLD
ControlPoint • Axceler • www.axceler.com
SILVER
Security Suite for SharePoint • TITUS • www.titus.com
BRONZE
Longitude Search for SharePoint and FAST • BA Insight • www.bainsight.com

Why It Won: Axceler's ControlPoint offers comprehensive management and control of SharePoint, enabling organizations to use SharePoint to its fullest extent without sacrificing security, compliance, or administrator sanity.

"On any given day," said Caroline Marwitz, senior editor at *Windows IT Pro*, "a single organization might use SharePoint for mission-critical capabilities such as records management and team collaboration sites, for extranet purposes such as creating portals for customers and clients, and for intranet purposes such as posting HR information and in-house application links. Axceler's ControlPoint solution helps organizations take advantage of SharePoint's Swiss Army knife capabilities, enabling SharePoint admins to take care of all aspects of a SharePoint implementation, offering control through permissions management, in-depth activity and storage analysis, content management, governance policy enforcement, and proactive management with alerts and scheduled analyses. As SharePoint use explodes in the financial, educational, government, life sciences, professional services, and energy sectors, ControlPoint lets admins help their organizations to get the most out of SharePoint while staying firmly within the boundaries of compliance."

Community Choice

GOLD
SharePoint Change Reporter • NetWrix • www.netwrix.com
SILVER
DocAve software for Microsoft SharePoint • AvePoint • www.avepoint.com
BRONZE
ControlPoint • Axceler • www.axceler.com

Other hot products in this year's survey . . .
AppAssure Software's DocRetriever
HP TRIM for SharePoint
Metalogix Software's StoragePoint

Best Security Product

Editors' Best

GOLD
QualysGuard Security and Compliance Suite • Qualys • www.qualys.com
SILVER
Enterprise Random Password Manager • Lieberman Software • www.liebsoft.com
BRONZE
Specops Password Reset • Specops Software • www.specopssoft.com

Why It Won: Qualys has emerged as a leading security vendor, and the QualysGuard Security and Compliance Suite is a major reason.

"With IT resources distributed throughout the cloud and in on-premises environments," says Jeff James, industry news analyst for *Windows IT Pro*, "finding a comprehensive security solution that can cover all the bases can be a challenge. Throw in auditing, compliance, and vulnerability assessment needs, and the task becomes even more daunting. That's where the QualysGuard Security and Compliance Suite enters the scene by providing a one-stop solution for all of these disparate IT security needs. A management console lets admins control all QualysGuard features from a single pane of glass, and extensive reporting features allow IT managers to receive the correct information when and how they want to receive it. SaaS security solutions are just beginning to gain traction in the market, and Qualys is blazing the trail."

Community Choice

GOLD
Symantec Endpoint Protection • Symantec • www.symantec.com
SILVER
Centrify Suite Platinum Edition • Centrify • www.centrify.com
BRONZE
Malwarebytes Anti-Malware • Malwarebytes • www.malwarebytes.org

Other hot products in this year's survey . . .
Cisco's Access Control Server
NetWrix's Change Reporter Suite
Avecto's Privilege Guard

"Reputation-based scanning is the future. Symantec Endpoint Protection's performance is amazing!"

Best Systems Monitoring Product

Editors' Best

GOLD
HP Operations Manager • HP • www.hp.com
SILVER
NetIQ AppManager Suite • NetIQ • www.netiq.com
BRONZE
Applications Manager • Zoho • www.manageengine.com

Why It Won: HP Operations Manager monitors pretty much everything you can think of in the data-center infrastructure.

"Vertically up the stack, HP Operations Manager monitors hardware components, VMware or Microsoft hypervisors, Microsoft and Linux/UNIX OSs, and the applications that run on them," says Sean Deuby, technical director for *Windows IT Pro*. "Horizontally across many types of hardware, it can also collect events from other event monitors or network, storage, or application components to be a manager of managers. I especially like the dynamic Services view of Operations Manager, where you can start with a top-level line of business service (such as Ordering) icon, and drill deeper and deeper into a complicated service hierarchy until you reach the actual systems themselves. Service interruptions deep in the hierarchy, though flagged themselves, don't necessarily cause the high-level service to be flagged; only if the interruption is detected to impact the entire service will the summary icon show a warning."

Community Choice

GOLD
HP Operations Manager • HP • www.hp.com
SILVER
Service Monitor • NetWrix • www.netwrix.com
BRONZE
NetIQ AppManager • NetIQ • www.netiq.com

Other hot products in this year's survey . . .
Zoho's Applications Manager
Nagios Enterprises' Nagios
Citrix GoToManage

"HP Operations Manager is comprehensive and dependable."

Best System Utility

Editors' Best

GOLD
Windows Sysinternals Suite • Microsoft • www.microsoft.com
SILVER
LogMeIn Pro • LogMeIn • www.logmein.com
BRONZE
Snort • Snort • www.snort.org

Why It Won: Quite simply, the Windows Sysinternals Suite is industry-standard perfection.

"The Sysinternals Suite is an essential collection of 67 system-troubleshooting tools that every Windows administrator should have," says Michael Otey, technical director for *Windows IT Pro*. "The depth and breadth of these tools is amazing. For example, tools such as Process Explorer and Process Monitor are easier to use and provide deeper insight into your running jobs than Windows' built-in tools. DiskMon lets you track your hard disk utilization, and RootKitRevealer shows any API discrepancies that might indicate the presence of a rootkit. If that wasn't enough, the ZoomIT utility is great for presentations, allowing you to magnify sections of your screen and even make simple drawings and annotations."

Community Choice

GOLD
Diskeeper • Diskeeper • www.diskeeper.com
SILVER
Disk Space Monitor • NetWrix • www.netwrix.com
BRONZE
Paragon Alignment Tool • Paragon Software Group • www.paragon-software.com

Other hot products in this year's survey . . .
Microsoft Windows Sysinternals Suite
Smith Micro Software's SendStuffNow
Scooter Software's Beyond Compare

"Diskeeper is the most simple and superb tool to have in your organization."

Best Task Automation Product

Editors' Best

GOLD
AutoMate • Network Automation • www.networkautomation.com
SILVER
Automation Anywhere • Automation Anywhere • www.automationanywhere.com
BRONZE
NetIQ Aegis • NetIQ • www.netiq.com

Why It Won: AutoMate continues to make automation application development intuitive and user-friendly, and has brought an array of new features to the table.

"IT professionals only have so much time in a day to dedicate toward a particular task," says Blair Greenwood, editorial assistant for *Windows IT Pro*. "IT pros need to find solutions that help streamline business processes. AutoMate helps users increase the speed and accuracy of business processes through task automation. The new version of AutoMate, AutoMate 8, includes task automation support for cloud-based SharePoint automation. Users can manage lists, list items, documents, and roles on any SharePoint server. In addition, AutoMate 8 supports task automation for VMware, Amazon Web Services, and Exchange 2010. AutoMate 8 is incredibly easy to use and features a revamped task builder that helps users create automation applications on the fly."

Community Choice

GOLD
Automation Anywhere • Automation Anywhere • www.automationanywhere.com
SILVER
NetIQ Aegis • NetIQ • www.netiq.com
BRONZE
AutoMate • Network Automation • www.networkautomation.com

Other hot products in this year's survey . . .
Siber Systems' RoboForm
Specops Software's Specops Command
Advanced Systems Concepts' ActiveBatch

Best Vendor Tech Support

Gold: Dell
Silver: Microsoft
Bronze: HP

Best Free or Open-Source IT Tool

Editors' Best

GOLD
Spiceworks • Spiceworks • www.spiceworks.com
SILVER
LogMeIn Free • LogMeIn • www.logmein.com
BRONZE
Dell KACE Secure Browser • Dell • www.dell.com

Why It Won: Spiceworks is a unique free tool that helps users complete an array of tasks, including network monitoring, UPS power management, Help desk solutions, and much more.

Justin Davison, senior systems engineer of IT operations at RJ Lee Group, uses Spiceworks for software compliance and change management. "We take advantage of the Spiceworks community as a great source of information, not just for solving problems that we're having but also to poke our heads up and see what other IT pros are doing and how they're handling different issues and situations." Davison said that his company often saves money by taking the community's ideas back to the organization. Davison also said Spiceworks provides a suite of tools that encapsulate day-to-day tasks. "In the past, I would look for free single-purpose tools and I would spend a lot of time trying to integrate them and keep them updated. Spiceworks really gives me a multi-tool instead of a screwdriver. It's become an absolutely critical piece of my IT infrastructure. I don't know how I would go back to not using it. If you asked me what to compare Spiceworks to, I would be comparing it to some pretty expensive software suites."

Community Choice

GOLD
Spiceworks • Spiceworks • www.spiceworks.com
SILVER
Google Apps • Google • www.google.com
BRONZE (tie)
Notepad++ • Notepad++ • www.notepad-plus-plus.org
Skype • Skype • www.skype.com

Other hot tools in this year's survey . . .
Malwarebytes
Centrify Express
AVG Technologies' AVG Free

Best Training and Certification Product or Service

Editors' Best

GOLD
Mountain View Systems' Certification Boot Camp • Mountain View Systems • www.mntview.com
SILVER
CBT Nuggets • CBT Nuggets • www.cbtnuggets.com
BRONZE
Transcender Test Prep Practice Exams • Kaplan • www.transcender.com

Why It Won: As certifications become increasingly important for displaying highly specialized knowledge to potential employers, Mountain View Systems' Certification Boot Camp remains one of the best programs to quickly study and take a certification exam.

For Rick Roach, infrastructure manager and communications manager for the City of Odessa, Texas, Mountain View Systems is his first choice for certification training every time. "I attended James [Carrion]'s very first class on NT 4.0 in Denver in 1998. James's teaching style and depth of knowledge is incomparable. I attended [Mountain View Systems] in Fort Collins, Colorado, for my MCSE upgrade to 2000 in 2001. Again there are no complaints. James's teaching method gives you everything you need to do the job. During this time, I received my Microsoft training certification and was teaching Microsoft certification classes at a New Horizons franchise I was a partner in. Every class I taught I tried to emulate James. He taught me a great deal about giving instruction and passing on knowledge. I would not really call his classes a boot camp because he covers everything and does not teach the test. I went to work as Network Manager at the City of Odessa, Texas, in 2002. I recommend Mountain View Systems to anyone wanting to learn to do the job. I send my people there now. I am scheduled to go back this November to refresh my Microsoft certifications. As a five-time returning customer, I can say they do it right!"

Community Choice

GOLD
TrainSignal Premium Computer Training Videos • TrainSignal • www.trainsignal.com
SILVER
Citrix GoToTraining • Citrix • www.citrix.com
BRONZE
HP ExpertONE • HP • www.hp.com

Other hot products in this year's survey . . .
SQLskills
Transcender's Test Prep Practice Exams
TestOut's LabSims

Best Virtualization Product

Editors' Best

GOLD
VMware vSphere • VMware • www.vmware.com
SILVER
DataCore SANsymphony-V • DataCore Software • www.datacore.com
BRONZE
Virtualization Manager • SolarWinds • www.solarwinds.com

Why It Won: Microsoft Hyper-V is coming on strong, but VMware vSphere still rules the virtualization roost.

"VMware has been leading Microsoft in the virtualization market for years," says Jeff James, industry news analyst for *Windows IT Pro,* "and vSphere 5 continues that tradition. Although Microsoft Hyper-V gets a massive upgrade in Windows Server 8, Microsoft's latest server OS won't be available until late 2012. VMware isn't standing still, so we'll likely see yet another revision of vSphere before the next Hyper-V hits the market. Can VMware hold off Microsoft's big push in the virtualization space? Time will tell, but VMware will likely remain the virtualization platform of choice for most businesses in the near future, and vSphere 5 should help VMware maintain its leadership position."

Community Choice

GOLD
Citrix XenServer • Citrix Systems • www.citrix.com
SILVER
VMware vSphere • VMware • www.vmware.com
BRONZE
VMware Change Reporter • NetWrix • www.netwrix.com

Other hot products in this year's survey . . .
VMware Workstation
VMware ESXi
Citrix XenDesktop



InstantDoc ID 140879

Paul Thurrott...



. . . he's not in Microsoft's pocket, but now he can be in yours.

The independent voice for IT enthusiasts

Paul Thurrott delivers news, tips, commentaries, and reviews on Microsoft technology – from gaming to mobile to servers to software, and coverage of Microsoft competitors in between. Get daily updates without reaching farther than your pocket.

Download your
Paul Thurrott: PocketTech app today

windowsitpro.com/mobile-apps

Available for iPhone | Windows Phone 7 | Android

Windows IT Pro Congratulates **AvePoint**

AvePoint®

Your SharePoint.® Our Innovation.



Category: **Deployment/ Configuration**

Product: **DocAve Deployment Manager**

Award: **Editors' Best Silver**



Category: **SharePoint**

Product: **DocAve Software Platform for Microsoft SharePoint**

Award: **Community Choice Silver**

Learn more about AvePoint here: www.avepoint.com • 201.793.1111

Proven Leader in Governance **Solutions** for **Microsoft Sharepoint**



Migrate. Integrate. Manage. Optimize. Protect. Report.

Backed by Global, Live 24/7 Support

Passion. Dedication. Excellence.

Powered by one of the world's largest SharePoint research and development forces located across 4 continents, 10 countries, 19 cities.

AvePoint®

Your SharePoint. Our Innovation.

www.avepoint.com

FEATURE

Windows 8 A Sneak Peek at Microsoft's Newest Client OS

The Developer Preview reveals huge changes for both devs and users

by Paul Thurrott

At Microsoft's first BUILD Conference in September 2011, the software giant finally took the wraps off Windows "8" (yes, it's still a code name) and described its vision for the future of PC computing. And although this upgrade doesn't appear to be too compelling for businesses, compared with Windows 7, I think Microsoft has hit the right balance and will see huge success with consumers and individuals that will put a serious dent in the momentum of Apple's iPad. The only problem? Windows 8 isn't expected until at least mid- to late-2012.

What Is It?

Windows 8 is the next major version of Windows on the desktop and the successor to Windows 7. From a user experience perspective, Windows 8 combines the interfaces and terminologies from Windows Phone 7 with the now "classic" desktop UI of Windows 7, providing a somewhat jarring experience when you navigate between apps that run in the two experiences.

The new Windows shell provides a Metro-style UI called the Start screen, which is what Microsoft describes as "touch first." This means that it's designed with multi-touch in mind, and it works wonderfully on touch-capable screens such as those that will be included on a coming generation of iPad-like slate PCs. But the new shell also works well with keyboard and mouse, and, for you tablet PC holdouts, with a stylus as well.

Although many will confuse this distinction, the new shell (i.e., the Start screen) isn't an app, or layer, on top of the old Windows desktop. It is in fact the shell, both logically and literally. You can still access a mostly complete Windows desktop, along with any now-legacy applications that run in that environment. However, that desktop is subordinate to the new shell. In fact, as far as the new shell is concerned, the desktop is just another app.

What makes this possible is a completely new Windows runtime called Windows Runtime (WinRT). This runtime replaces Win32, which was itself based on the so-called Win16 runtime that literally dates back to the first version of Windows in 1985. So these things don't change very often.

WinRT provides APIs and classes that mimic what Microsoft previously provided in .NET, so they're logical, well-constructed, and well-understood by modern developers. But unlike .NET, WinRT isn't a layer on top of other technologies, or an abstraction of any kind. Instead, WinRT sits directly on the NT kernel and is the lowest-level way for developers to access new Windows features. Unlike previous shells and environments, however, WinRT is unique in that it provides developers with the same capabilities via web standards technologies such as HTML5 (HTML, CSS, and JavaScript) as it does via more traditional languages (e.g., C#, C, C++, Visual Basic) and presentation layers (XAML).

When Microsoft says it's "reimagining" Windows with this release, for once it's not hyperbole. For developers, Windows 8 brings a major new runtime and API set with the capabilities exposed by a new shell. For users, it brings a completely new and beautiful user experience that's as at home on iPad-like slates as it is on more traditional PCs. Users haven't had a change like this since Windows 95, and developers haven't seen a similar sea change since .NET a decade ago. The fact that Windows 8 affects both groups in equally seismic ways is proof positive of its importance. Windows 7 was about fixing what was wrong with Windows Vista and fine-tuning a stable base; Windows 8 is about surging ahead.

The New User Experience

How different is Windows 8 from its predecessors? Let's start with boot time. Using a non-shipping developer prototype slate PC, I've seen boot times of about 5 seconds. On my own laptop, which isn't optimized for Windows 8, it's closer to 8 seconds when you factor out the dual-boot menu I've compulsively left in place "just in case."

After the blink-and-you'll-miss-it boot process, you're presented with your first UI, a full-screen Lock screen that displays a background photo, prominent time and date, and a variety of notification icons using a very Windows Phone–esque presentation. (Don't worry, that's a compliment.) You slide this screen up, using a finger swipe from the bottom of the screen or a right-click of the mouse, to log on. There are a couple of fun new ways to log on now in addition to traditional password: You can use a four-digit PIN password (as on a phone) or the new Picture Password, in which you use your own personally created sequence of taps and gestures over a personalized photo.

Your user account can be local and created as before, of course, or you can simply use your Windows Live ID. I suggest the latter, because this approach will autopopulate a lot of the upcoming integration with Windows Live services, such as mail, contacts, calendar, and online storage.

After you log on, you'll see the new Windows 8 Start screen. This screen, like Windows Phone's Start screen, provides several live tiles floating over a background, which in this case is called an Accent and can be customized with colors or background images. (This isn't in the Developer Preview, unfortunately, which is colored green for "Go.") These tiles are larger and more expressive than their Windows Phone cousins, and the user can control whether the tiles are small and square or large and rectangular on a per-tile basis. The tiles typically represent apps—either new Metro-style apps or traditional Windows applications—in addition to other items, such as Control Panels, contacts, email accounts or folders, and so on.

It's probably obvious that the new Start screen is a replacement for the Start screen in previous versions of Windows, but it's also a replacement for the taskbar in that it can be used for simple app switching. In this mode, you'd use Windows 8 like a phone, by launching and using an app and then tapping the Windows key on the PC—or keyboard—to return to the Start screen and then launch another app.

The Start screen is fast, fluid, and surprisingly responsive. You can flick left and right through various screens full of tiles, in either landscape or portrait mode (virtually all Windows 8 apps can be used in either orientation), group the tiles, and optionally name those groups. (This feature is currently missing in Windows Phone, although these two platforms will supposedly merge in Windows Phone 8 late next year.)

Windows 8 also supports a system-wide set of Charms that sit hidden on the right edge of the screen; just swipe in from the right to display the list, which includes Search, Share, Start, Devices, and Settings. These Charms are accessible everywhere, from the shell/Start screen, from within any app, and from the classic desktop. There's also a nice time/date overlay that appears when the Charms are displayed.

A New Generation of Tailored Apps

The apps that run under the new shell are described as "tailored" or "immersive." They always run full-screen, although Microsoft provides a way to show two apps (a pair of tailored apps or one tailored app and one desktop app) side by side. So far, the sample and built-in apps we've seen are fairly basic, leading to another Windows 8 misconception that these apps can provide only simple UIs—which isn't the case. Yes, there will be tons of simple Twitter and weather apps, but Microsoft is also looking at porting its Office suite to the new shell, and I've been told to expect some amazing third-party apps well before the product's launch next year.

Because this is Windows, you can of course multitask between apps (and desktop apps), and you can use old keyboard shortcuts such as Alt+Tab (Windows Flip) to switch between them. The new shell sports a new way of switching between apps, however, which involves swiping from the left edge of the screen toward the center. If you do so slowly, you can dock, or Snap, the "next" app next to the current app, visually. Or you can swipe rapidly to move between the various running programs more quickly.

Metro-style tailored apps (but not legacy Windows apps) share some interesting properties. When they're not onscreen, they're suspended, which dramatically drops memory usage. Over time, suspended apps are automatically killed by the OS if the RAM they use is needed, as on a phone. And users won't typically quit these apps, as they do today with traditional applications; that's handled by the OS too. (You can use Task Manager to kill Metro-style apps if you're the micro-manager type.) In addition, these apps can't display a Save dialog or similar interface—and because they can be killed at any time, they must save any state and date automatically on an ongoing basis.

Metro-style apps support the notion of an Edge UI. Swiping up from the bottom or down from the top of the screen (or right-clicking with a mouse) brings up hidden controls in the form of an App Bar (found on the bottom of the screen) and, optionally, top-mounted controls. In the immersive version of Internet Explorer (IE) 10, for example, the Edge UI consists of an address bar and browser buttons on the bottom and a set of tabs on the top.

To make developers happy and to make it easier for users to find and install new apps, Microsoft is creating a new Windows Store for Windows 8. (It's not in the Developer Preview build.) Similar in appearance and utility to the Windows Phone Marketplace, the Windows Store comes with several advantages for everyone. First, it's curated by Microsoft and will therefore sell only safe, well-written apps that pass stringent tests. Second, it will offer both new, Metro-style apps and legacy Windows applications, although the latter are listing-only; developers will have to host the downloads themselves. Microsoft claims that all Metro-style apps will install in just 2 to 3 seconds—but we'll see.

Although Microsoft hasn't announced licensing for the store, I expect the company to offer the same 70/30 split on earnings for new apps and allow installation on four Windows PCs. Microsoft has stated that it won't charge a fee for listing legacy apps.

Windows 8 doesn't currently come with many built-in immersive apps, so Microsoft is bundling numerous sample apps, which I don't expect to be present in the final version of the OS. (The company will likely offer them via download.) But the shipping version will include Internet Explorer, Messaging, Music, and Video; Windows

Live will supply awesome full-screen Mail, People (contacts), Calendar, (Video) Chat, Bing, Photos, and other apps. It's unclear if these will be built-in or require a visit to the Windows Store and/or Windows Update.

As per the Windows 7 taskbar, the Start screen holds only a subset of available apps. Curiously, there's no obvious full list of available apps. However, if you tap the Search Charm from the Start screen, you'll see a list of all your apps there. You can also search for new apps and traditional desktop apps from this interface, although the latter option is incomplete; it couldn't find things like Disk Management for some reason.

Cloud Integration

It's going to be a while before the full depth of Windows 8's cloud integration bits is well-known. But aside from the aforementioned Windows Live ID integration for logging on, there are some pieces available in the Developer Preview and some news about other features coming in the future.

Windows Live SkyDrive, previously a forgotten wasteland among Microsoft's consumer-oriented cloud services, will finally see deep integration with Windows 8. In the past, we expected that integration to come via Windows Explorer–based access to SkyDrive's voluminous 25GB of storage—but with the classic desktop on the on-ramp to obsolescence, it's understandable why that's not happening. Instead, Windows 8 apps will integrate with SkyDrive and, via a new system-wide File Picker (analogous to the Open dialog in previous Windows versions), you'll be able to access your SkyDrive folders and files from the PC just as you do with local resources.

Microsoft is also providing some interesting new capabilities around backup and restore, including a new PC Refresh option that will let you wipe out Windows without killing any of your settings and customizations, immersive apps and app states, and data files. This information is actually stored on the PC's hard disk and will survive the reinstall process—which takes just 4 to 5 minutes—but there's some evidence that this information will be stored in SkyDrive too, which opens the possibility that you'll be able to log on to any Windows 8 PC with your Windows Live ID and immediately access your custom PC environment.

One feature that will be included in Windows 8 is the ability to browse the hard disks of any of your other Windows 8 PCs using the web-based SkyDrive interface. This will let you seamlessly access your home PC when you're traveling, or your work PC from home.

And finally, although this isn't exposed on the current Developer Preview build, I've seen other builds internally at Microsoft that feature SkyDrive integration with Windows Backup. This suggests that you might be able to actually back up a PC to the cloud using only Microsoft solutions, although it's unclear whether this feature is as I've described and how Microsoft will handle storage above 25GB. Stay tuned.

New Platform Features

With Windows evolving into a more secure environment in Windows 8 and picking up device-like reliability in the process, Microsoft is starting to think in terms of "Windows devices" rather than Windows PCs. And a big part of that experience, of course, involves instant wake and sleep times, both of which are part of the plan for Windows 8. There are various aspects to how Microsoft plans to achieve these goals, but a big part involves new power management capabilities, the most notable of which is a new power management called Connected Standby, which requires new Intel (or ARM) chipsets. Connected Standby is essentially the type of sleep you get with an iPad or other device: It uses very little power and can remain in this state for several weeks, not several days. But when you come back and tap the power button, the machine springs to life instantly.

After years of me begging and pleading (no, I don't really believe I had any influence), Microsoft is finally adding antivirus capabilities to Windows 8, in addition to preexisting anti-malware technologies. This will be surfaced by the newly resuscitated Windows Defender, which appears to have eaten Microsoft Security Essentials whole. And Microsoft's successful SmartScreen anti-malware scanner, which uses behavioral and reputation-based techniques, is being extended from IE to Windows Explorer so that it works everywhere.

Speaking of Defender, the version supplied in Vista had excellent startup application control, but this functionality was stripped out in Windows 7 for some reason. In Windows 8, it's back, although it can be found in Task Manager now. Note, though, that immersive, Metro-style apps *cannot* be launched at startup; this capability applies only to legacy Windows applications.

There are some neat device integration bits, as expected. Windows 8 works with modern interface standards such as USB 3.0, of course, and with all the devices that work with Windows 7. But Microsoft is abstracting print drivers further in this release and currently supports over 70 percent of all available printers via a new Printer storage class. (More are expected by launch.) And this isn't basic functionality: The printer makers' custom and advanced functionality is exposed through the new immersive interfaces as well.

Using the Desktop

Tap the Desktop tile on the Start screen and you'll be confronted with the traditional Windows desktop you know and love, albeit with a few changes. Microsoft has detuned the "gleam" effect on the taskbar because it was apparently egregiously unfriendly to power management in Windows 7 and Vista, although there's a good possibility this will be tweaked further before final release. (Microsoft is experimenting with different taskbar designs, including a black version that won't make the cut.)

The Start button has been redesigned and no longer launches a Start menu; instead, you're returned to the Start screen. This will be disconcerting at first, but the bigger issue is that the loss of the Start menu also means you lose such things as a way to navigate through a list of all installed (legacy) applications, easily find Control Panels, and use Start Menu Search. Keyboard commands (e.g., WINKEY+R for the Run box) still work, of course, but it's not a complete solution. Hopefully, this will be fixed before the final release.

The Windows desktop has gotten a few upgrades—surprising, given all the emphasis on the new shell. Windows Explorer gets a complex new Ribbon-based UI (don't worry, you can hide it), and file copy has been overhauled completely so that it's much faster, and multiple file copies now use a single dialog. Amazingly, Microsoft has significantly improved Windows 8's multi-monitor capabilities as well.

Windows 8 for Business Users

For the business user, Windows 8 represents more of an evolutionary step than a big leap forward. Most businesses will probably opt to hide the Start screen and use the old desktop interface, because the Windows 8 desktop is reasonably identical to that of Windows 7 and won't require retraining. And I've been told that admins won't be able to granularly control the Start screen and immersive apps at all, which might limit that environment's appeal further. (I'll need to confirm this in the future, because the current builds are incomplete.)

From a user experience and deployment standpoint, Windows 8 is largely identical to Windows 7. This will likely be cheered by many admins, especially those who are well along in their Windows 7 deployments. For those environments, I recommend proceeding; there's no reason to wait for Windows 8.

That said, there are a few new business-oriented features in Windows 8. It includes Client Hyper-V, which is a full-blown client-side version of Microsoft's powerful hypervisor-based virtualization solution and appears to look and work identically. It's been updated to support power management (a key issue for those who wanted to use Windows Server 2008 R2's Hyper-V on a laptop) and replaces the old-fashioned Windows Virtual PC we currently use.

A new feature called Windows To Go lets you run Windows 8 from a secure, BitLocker-protected USB memory key instead of a PC's local storage. This can be useful in many situations, and it can be configured to reset to a factory-fresh condition each time the key is removed. For customers looking at expensive and complex Virtual Desktop Infrastructure (VDI) solutions, this could be a godsend.

Finally, Remote Desktop is overhauled in Windows 8. It gets the Metro treatment and a new multi-machine interface.

The ARM Conundrum

If there's anything confusing about Windows 8, it's how Microsoft intends to support and sell the various ARM-based flavors of the OS. Currently, desktop versions of Windows run on the Intel-compatible x86/x64 platform, which has been a consistent situation for many years. But with Windows 8, Microsoft will also sell versions that run on ARM chipsets for the first time.

The ARM versions of Windows 8 will each be custom made for a particular ARM chipset and will be sold only with ARM devices, and not as software-only packages. These ARM versions of Windows 8 will run the entire body of immersive, Metro-style apps that developers will have already started creating by the time you read this. Every one of these apps will run on both ARM and x86/x64 versions of Windows. The ARM versions of Windows will *not,* however, run legacy Windows applications, including Microsoft Office 2010 (which Microsoft perplexingly demonstrated back in January; my guess is this was a bid to prove that ARM versions of Windows 8 would be "real" Windows versions).

There's some speculation about whether the classic Windows desktop environment will be available on ARM versions of Windows. My gut says it will have to be, but I could see Microsoft not providing this environment at all because the ARM versions of Windows are aimed at a very specific market: thin, light, and battery-friendly devices such as the iPad.

What's odd about this situation is that Microsoft and its partners will be selling two somewhat incompatible platforms, both of which will be marketed as Windows devices. Those running Intel-compatible x86/x64 chipsets will run classic Windows applications and offer the "full" PC experience, whereas those running on ARM won't run classic Windows applications and will be more device-like.

Further confusing matters is that Intel is racing to develop ARM-like versions of its "Sandy Bridge" chipsets that will allow PC makers to build and sell tablets, Ultrabooks, and other PCs that could be as thin, light, and battery friendly as ARM designs. These chipsets and machines should absolutely be ready in time for Windows 8 to ship in mid- to late-2012. So Microsoft must have some idea about how it will market these similar but different products—but the company is remaining mum about its plans.

Availability and Requirements

The Windows 8 Developer Preview is available for free from the BUILD Windows website (www.buildwindows.com). It comes in versions for Intel-compatible x86/x64 PCs only, and not ARM devices. There are 32-bit (x86) and 64-bit (x64) versions, as well as a special x64 version that includes developer tools (prelease versions of Visual Studio 11 and Expression Blend 5, among others).

Windows 8 comes with the same hardware requirements as did Windows 7, so it will run on any PC that was made in 2005 or later. In fact, Windows 8 uses fewer resources than Windows 7, so some users might even experience better performance on the same hardware. That said, I don't recommend the Windows 8 Developer Preview to casual users because the software is buggy and incomplete. A wider beta version should appear by January 2012 and be feature complete.

Final Thoughts

I die a little bit every time a Microsoft representative uses the term "reimagining Windows," but let's give Microsoft some credit here. Windows 8 really is a fresh new start for Windows, and that's equally true for both users and developers. The fact that Windows 8 was designed before the iPad was revealed only underscores that Microsoft isn't as far behind as some people think when it comes to anticipating consumer trends. However, the fact that Windows 8 won't be delivered to us until next year means the next several months are going to be quite painful.

And that's what's special about Windows 8. It makes what I'm using now seem shabby by comparison. I can't think of a greater compliment than that, especially when what I'm using now—Windows 7—is so refined and successful. Improving on Vista was easy—a sure thing. But Windows 8 is the real achievement of Microsoft's Sinofsky era and the start of a new decade of touch-friendly, mobile, and connected computing. It's still early, but Windows 8 looks incredible.

InstantDoc ID 140964



Paul Thurrott
(paul@windowsitpro.com) is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows (winsupersite.com), a weekly editorial for Windows IT Pro UPDATE (www.windowsitpro.com/email), and a daily Windows news and information newsletter called WinInfo Daily UPDATE (www.wininformant.com).

FEATURE

Active Directory Replication Topology

Efficiently manage replication across site boundaries

by Brian Desmond

In "Active Directory Replication In Depth" (August 2011, InstantDoc ID 135815), I discussed the specifics of Active Directory (AD) replication technology with regard to how objects and attributes are actually kept in sync and how changes to them are tracked. A layer above this is the discussion of how AD decides which domain controllers (DCs) should replicate with one another.

AD includes a very efficient background process known as the Knowledge Consistency Checker. The KCC is responsible for consuming information that administrators provide to AD in the form of subnets, sites, site links, and site link bridges to determine the best overall topology of connections between DCs. These connections are represented by connection objects, which the KCC automatically adds and removes as necessary. Your sites, site links, and site link bridges typically map closely to your network topology to form what's called a site topology. Figure 1 shows a sample site topology.

Site Topology Components

A site topology consists of sites, site links, and site link bridges.

Sites. Sites are a key part of your AD configuration, used not only for replication but also by clients and applications. Clients and applications use site information to find the DC or another resource that's logically closest to them on the network. To associate themselves with the correct site, clients depend on accurate subnet information in AD. Subnet information is defined in terms of IP subnet (IPv4 and/or IPv6) objects stored in the directory, which are in turn associated with sites.

In small environments with only a few sites, it's typically easy for administrators to keep subnet information up-to-date. But this task can be a challenge in large environments if there are frequent network changes and processes aren't in place to communicate these changes to AD administrators. When subnet information isn't up-to-date in AD, clients might be redirected to DCs that are across distant or slow WAN links, which leads to suboptimal performance at best. If your AD needs only one site, there's no need to define any subnets in AD.

Sites typically represent a group of well-connected subnets that contain one or more DCs. The definition for well-connected is very loose, although I like to use a minimum of a 10Mbps connection as a baseline. Sites typically (but not always) map directly to physical locations within your network; these locations contain DCs, as Figure 2 shows. A notable urban legend concerns the initial site that comes with a new AD forest: the Default-First-Site-Name site. Contrary to popular opinion, it's perfectly safe to delete or rename this site object depending on your requirements. There's no need to retain it as an empty site if you're not using it, or to not rename it if another name makes more sense.

In Figure 1, a company has offices in St. Louis and Detroit, but its DCs are located in Chicago. In this scenario, a single site is created for Chicago, but the subnets used in St. Louis and Detroit are

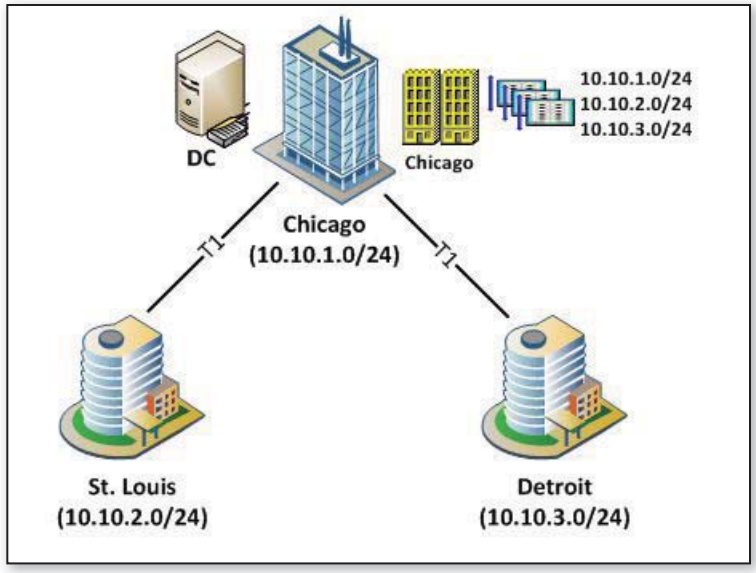


Figure 1: Sample site topology

associated with the Chicago site (in addition to the subnet for Chicago).

Although it's common to only create sites when there's a DC at that location, some applications, such as Distributed File System (DFS) and Microsoft System Center Configuration Manager (SCCM), take advantage of site information. For example, if you have an SCCM server at a location that doesn't have a DC, you'll probably need to create a site. When a site doesn't contain a DC, AD uses a process called automatic site coverage to determine which DCs clients in that site should use.

In Figure 2, the organization has offices in Seattle, Los Angeles, and San Diego. DCs are located in Seattle; however, an SCCM server also exists in San Diego. To ensure that San Diego clients connect to their local SCCM server, a site for San Diego is created and the San Diego subnet is associated with it. A second site for Seattle is created that contains the Seattle DCs, as well as the subnets for Seattle and Los Angeles.

Site links. We've discussed sites and the subnet objects that describe which clients should associate with that site—but we haven't discussed how sites are connected in AD. AD connects sites using site links. Site links frequently model your WAN topology. Site links contain two or more sites, and they model the paths replication can take, as well as influence client decisions around logically closest DCs and other servers. Although it's possible to connect more than two sites with a site link, site links are typically easier to manage if you stick with defining point-to-point site links (i.e., site links with only two sites in them).

Site links have several properties that you can tweak in addition to the sites contained within the site link. These properties include cost, replication frequency (how often replication occurs over the site link), and replication schedule (when replication can begin). Cost is probably the most misunderstood property of site links.

AD factors cost into decisions only when there are multiple paths between any two sites. If there's only one path, then cost doesn't matter because it's mandatory to use that site link. The value for cost also isn't particularly important as long as the preferred path is a lower cost than other paths. If you do need to set site link costs, there are a few strategies for doing so. The first strategy is to use values that are proportional to WAN link speed. You can find a table at briandesmond.com/blog/active-directory-site-links-naming-costing that makes a good cheat sheet if you opt for this approach. Another common strategy is to use static values for different types of connections. For example, connections between data centers have cost 100, connections between data centers and spokes have cost 200, and connections between spokes have cost 300.

Figure 3 shows a simple scenario in which site link cost doesn't matter. In this example, we have three AD sites: New York, Boston, and Atlanta. WAN links exist between New York and Boston, as well as between New York and Atlanta. Using this information, site links were created to model the WAN topology. Because there's only one path between each site, the costs on the site links are irrelevant.

Figure 4 shows a scenario in which site link costs do matter. In this scenario, each of the three sites is connected with a WAN link. Using this information, site links were created linking each of the three sites in a full mesh topology. Costs were set such that the links between Houston and Dallas and Houston and Austin are preferred over the link between Dallas and Austin.

In addition to cost, site links also have frequency and schedule properties. The

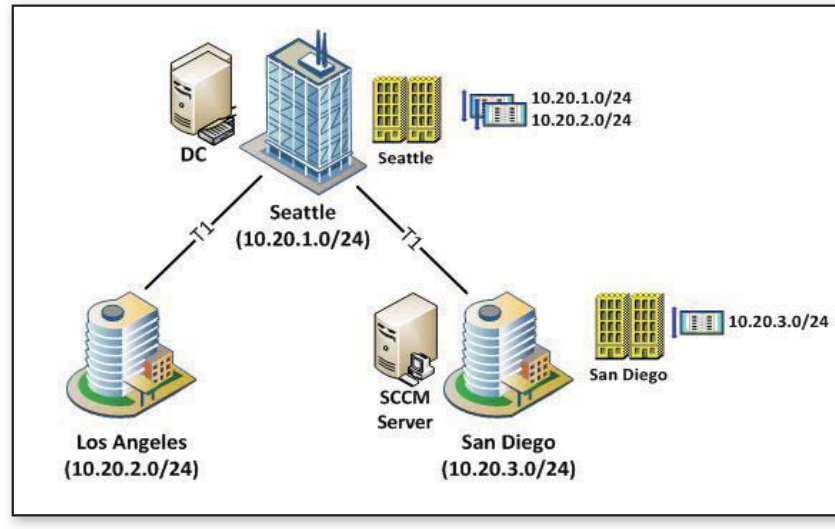


Figure 2: Sample site topology with auto site coverage

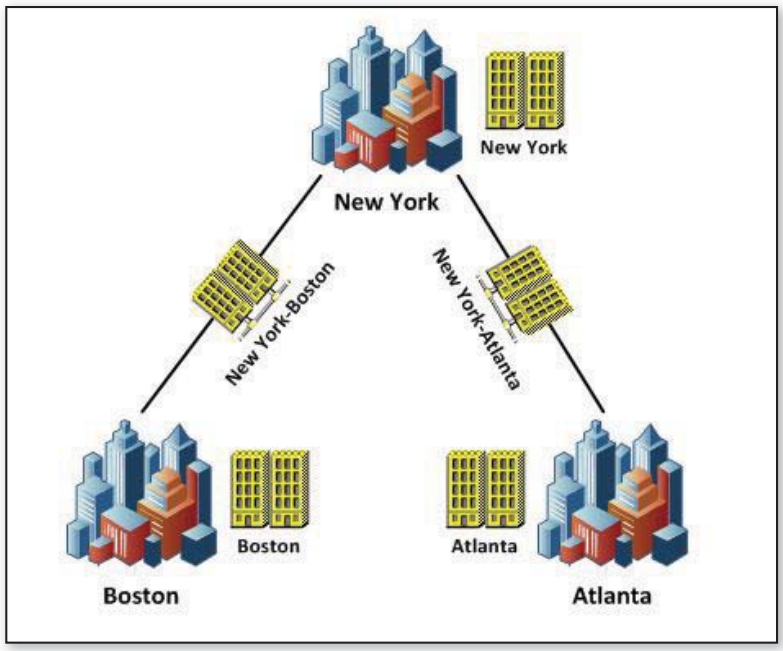


Figure 3: Site link costs not relevant

frequency is fairly straightforward in that it defines how often AD will initiate normal replication over the site link. This value can be as low as 15 minutes or as high as 1 week. If you need replication to occur more frequently than every 15 minutes, you can enable change notification for the site link by following these steps:

1. Launch ADSIEdit (Select Start, Run, ADSIEdit.msc).
2. Browse to \Configuration\Sites\Inter-Site Transports\IP.
3. Right-click the site link you want to edit, and select Properties.
4. Double-click the Options attribute.
5. Add 1 to the value displayed. If the value is null, set it to 1.

Change notification will cause AD to enable intra-site style replication over the site link, which will lead to synchronization occurring almost in real time. This change is typically made for site links that connect data centers.

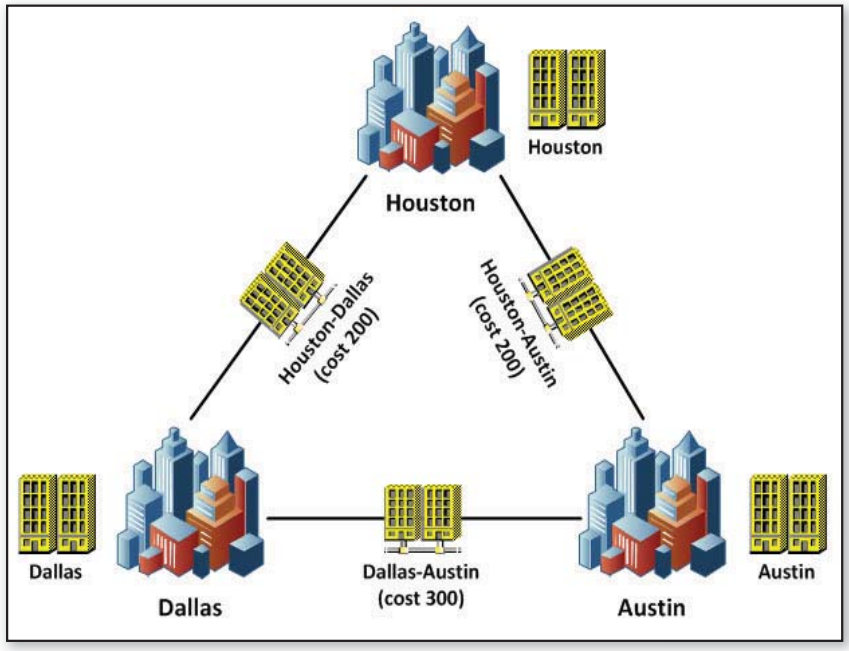


Figure 4: Site links with cost information

Learning Path

Windows IT Pro Resources

"Troubleshooting Active Directory Replication," InstantDoc ID 129333

"Active Directory Replication In Depth," InstantDoc ID 135815

Microsoft Resources

"What Is Active Directory Replication Topology?" technet.microsoft.com/en-us/library/cc775549(WS.10).aspx

"How Active Directory Replication Topology Works," technet.microsoft.com/en-us/library/cc755994(WS.10).aspx

"Troubleshooting Active Directory Replication Problems," technet.microsoft.com/en-us/library/cc738415(WS.10).aspx

Finally, the schedule defines when (i.e., during what time) Windows replication can begin. By default, the schedule allows replication to begin at any time; however, you might have a scenario in which you don't want to use a WAN link during certain times—possibly because of utilization, or for other reasons. A key data point around the replication schedule is that the schedule defines when replication can begin. After replication begins during the scheduled window, it won't stop until it's finished.

Now that we've looked at a few examples, let me highlight two final tips about site links that relate to naming and the default site link. One handy way to name site links is to name the link according to the two connected sites (e.g., New York-Boston), and then reverse the order in the Description field (i.e., Boston-New York). This approach lets you sort on either column in the Microsoft Management Console (MMC) Active Directory Sites and Services snap-in, depending on how you need the data presented. When a new AD forest is created, an initial site link is provisioned called the DEFAULTIPSITELINK. Much like the initial default site, you can rename or delete this site link if doing so makes sense.

Site link bridges. The final component of AD site topology is undoubtedly the least used. This component is known as the site

32%
INCREASE IN SYSTEM SPEED

Diskeeper®

Optimum system performance. Always.™

Diskeeper software owners were surveyed by Windows® IT Pro and the results revealed 14 critical areas of significant improvement in overall system efficiency. An average 32% boost in speed was just one of them. You can get similar results. Read the report at www.diskeeper.com/speedreport

"We have seen a 45-50% performance enhancement in read access and a 60-65% in write access….After installing Diskeeper, backup times were reduced by several hours, and user 'slowness' complaints went away."
– *American Imaging Management*



Innovators in Performance and Reliability Technologies®

Get Diskeeper FREE for a month at:
www.diskeeper.com/speed

1-800-829-6468

© 2011 Diskeeper Corporation. All Rights Reserved.

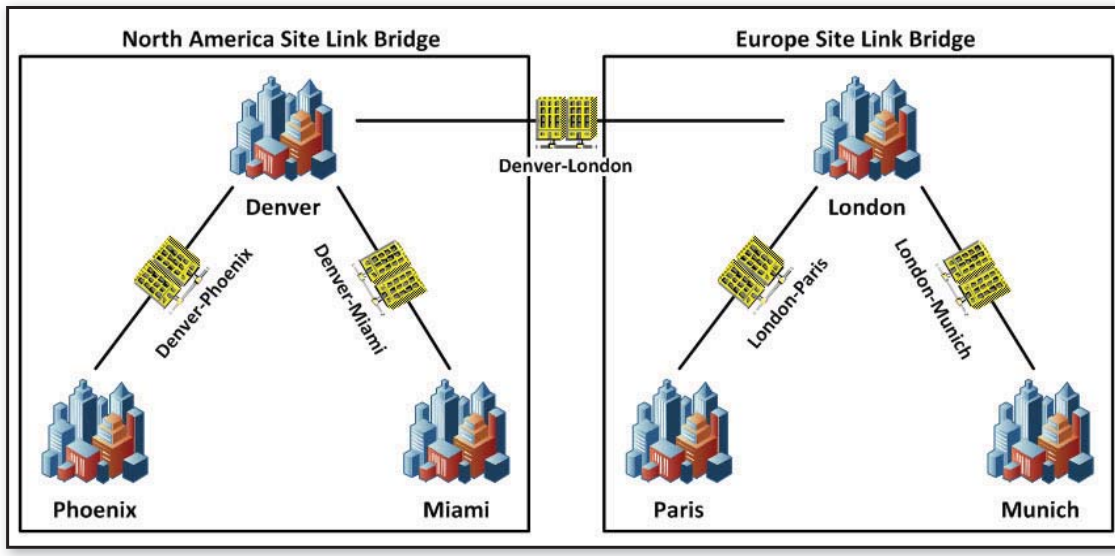


Figure 5: Site link bridges

link bridge. Site link bridges are used when you have a network that isn't fully routed. When your network is fully routed, a client (or server) on any part of the network can connect to a client (or server) on any other part of the network (with the exception of firewalls blocking this action). A common situation in which you might not have a fully routed network is if you have branch offices and it isn't possible for one branch office to communicate with another branch office over the network. Another scenario is when sites in one region can't connect to sites in another region.

By default, a setting called Bridge All Site Links (BASL) is enabled in AD. With BASL enabled, a DC in the Boston site (see Figure 3) can replicate directly with a DC in the Atlanta site, bypassing any DCs in New York, even though there's no site link connecting Boston and Atlanta. If this isn't possible in your network, you'll need to disable BASL. With BASL disabled, you can use site link bridges to define sets of site links that are fully routed.

In Figure 5, the only possible path over the network from North America to Europe is between servers in Denver and London. Within each region, there's full mesh connectivity over the WAN. To represent this in AD, it's necessary to create two site link bridges—one for North America and one for Europe. The North America bridge contains the Denver-Phoenix and Denver-Miami site links, whereas the Europe bridge contains the London-Paris and London-Munich site links.

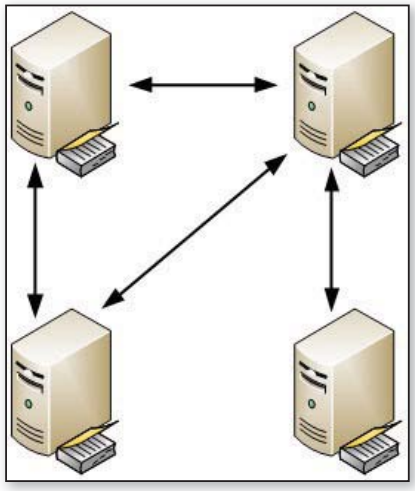


Figure 6: Intra-site replication topology

Creating Replication Connections

After you define your site link topology in AD, AD still needs to do some work to determine which DCs will replicate with one another. This calculation is performed in the background by the KCC. Two different topologies are calculated, leading to the overall replication topology. The first topology is for intra-site replication. Intra-site replication is replication between DCs that are in the same AD site. With intra-site replication, the KCC doesn't need to worry about things like site links and site link bridges because all the DCs are considered to be well connected. With this in mind, the KCC calculates a topology that's centered around ensuring that no DC in a given site is more than three hops away from any other DC in the site. This ensures that DCs within a site can converge and be in sync within about a minute (this time used to be about 15 minutes in Windows 2000 forests). Figure 6 shows a sample topology with four DCs in a site, considering the three-hop rule.

Inter-site replication topologies are calculated according to the site topology information that's included in AD. The calculation of inter-site replication topologies is performed by the Inter-Site Topology Generator. The ISTG is a component of the KCC that runs on one DC in each AD site and is responsible for creating connection objects for replication across site links.

Efficient Topologies

AD is very adept at calculating replication topologies within an AD site—but to replicate across site boundaries, administrators must provide information so that AD can select the best path. This information is provided in the form of sites, site links, and site link bridges that typically closely mirror the organization's WAN topology. With this information, the KCC and the ISTG can create efficient replication topologies for the forest.

InstantDoc ID 140895



Brian Desmond
(brian@briandesmond.com) is a Directory Services MVP and senior consultant for Moran Technology Consulting in Chicago. Brian is author of *Active Directory,* 4th edition (O'Reilly), and blogs at www.briandesmond.com. He wrote this article on his way to Santa Barbara.

35%
VIRTUAL SYSTEM SPEED BOOST

V-locity® 3
Virtual platform disk optimizer™

V-locity 3 prevents I/O bottlenecks no other technology can touch—increasing read/write speeds on host and guest systems by 35% or more. V-locity® virtual platform disk optimizer goes even further by ensuring automatic optimization creates no resource conflicts, even at the SAN level. It also eliminates disk bloat, economizing data storage. Read the report at www.v-locity.com/speedreport

"V-locity immediately went to work after installing it on our guest systems. Without touching the product, other than to view a 'before' image of the disk utilization, file access times and boot processes were improved within 24 hours and the changes were noticeable to end-users."
– *Synergy Solutions, Inc.*

Diskeeper corporation

Innovators in Performance and Reliability Technologies®

Get V-locity 3 FREE for a month at:
www.v-locity.com/speed

1-800-829-6468

© 2011 Diskeeper Corporation. All Rights Reserved.

Windows IT Pro Magazine Congratulates **Axceler**

Axceler

Windows IT Pro magazine

Editors' Best Awards



Company: **Axceler**
Category: **SharePoint**
Product: **Axceler ControlPoint**
Award: **Editors' Best Gold**



Company: **Axceler**
Category: **SharePoint**
Product: **Axceler ControlPoint**
Award: **Community Choice Bronze**

Learn more about Axceler here: www.axceler.com • 866.499.7092

Even our thumbs are happy!



Axceler

ControlPoint, the leading governance product for Microsoft SharePoint, is the proud winner of three prominent awards in 2011:

1) **2011 Windows ITPro Editors' Best Gold Award**, SharePoint Product Category
2) **2011 Community Choice Bronze Award**, SharePoint Product Category
3) **2011 Best of Connections Winner**, SharePoint Product Category

Get ControlPoint for your

- SharePoint Governance Policies
- SharePoint Security
- SharePoint Administration
- SharePoint Reporting and Analysis

Microsoft SharePoint 2010

Microsoft GOLD CERTIFIED Partner

Editors' Best GOLD

Best of tech·ed 2009

No Budget for Travel? No Problem!

Get the training you need right at your desk with

eLearning Courses

http://elearning.left-brain.com

Join industry experts for informative eLearning courses.
Each course includes in-depth sessions as well as live Q&A.

Our eLearning Series provides you with in-depth training on a variety of topics ranging from:

- Upgrading to SharePoint 2010
- Identity Management
- SQL Server for Non DBAs
- The Science of Great UI
- Administering SharePoint with Windows PowerShell
- And Much More!

Don't miss this opportunity for the training you need from the comfort of your own computer.

Check out the eLearning Series offerings today!

http://elearning.left-brain.com

Windows IT Pro SharePoint Pro SQL Server magazine DevProConnections

Windows Server 2008 R2 Firewall Security

Best practices for enabling a firewall in a production environment

by Alan Sugano

Today's security model is all about layers. If your network suffers a breach, security layers can at least limit the scope of the attack or slow down the hacker. In my experience, Windows Server 2008 R2 and Windows Server 2008 are the first versions of Windows Server in which you can successfully keep your firewall enabled and still have the server work in a production environment. The Microsoft Management Console (MMC) *Firewall with Advanced Security* snap-in is key to this capability.

Firewall Profiles

There are three different Windows Firewall profiles that can be configured with a Server 2008 R2 firewall. Only one of these profiles can be active at a time.

1. Domain profile—This profile is active when the server is connected to an Active Directory (AD) domain via an internal network. This is the profile that's typically active, because most servers are members of an AD domain.
2. Private profile—This profile is active when the server is a member of a workgroup. Microsoft recommends more restrictive firewall settings for this profile than for the domain profile.
3. Public profile—This profile is active when the server is connected to an AD domain via a public network. Microsoft recommends the most restrictive settings for this profile.

When you start the *Firewall with Advanced Security* snap-in, you can view which firewall profile is active. Although Microsoft recommends that you can have different security settings based on the firewall profile, I typically configure the firewall as if a perimeter firewall doesn't exist. With this approach, if any ports are accidentally opened on perimeter firewalls, Server 2008's Windows Firewall will block the traffic. Just as with previous versions of Windows Firewall, all inbound connections are blocked and all outbound connections from the server are allowed by default in Server 2008 R2 (as long as there's no existing Deny rule).

With these settings, my organization's firewall configuration leans toward a public profile environment. When we create a rule, we make it active for all three profiles. By using a firewall configuration that's consistent across all three domain profiles, we don't have to worry about exposing any unwanted ports in case the Windows Firewall profile changes.

IPsec and Domain Isolation

You can implement domain isolation by using Windows Firewall's IPsec feature. Domain isolation prevents the communication of a non-domain computer from connecting to a computer that's a domain member. When communication is established between two domain members, you can configure the firewall to encrypt all traffic between the two computers with IPsec. This configuration

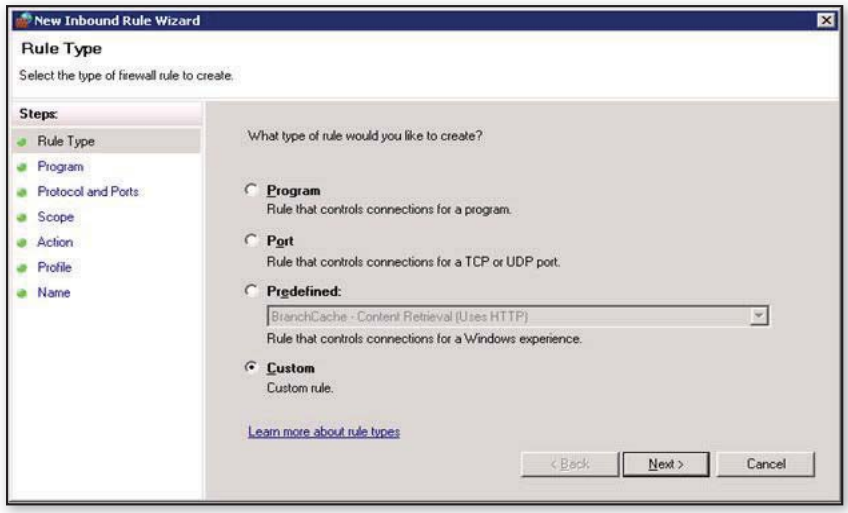


Figure 1: Creating a new inbound rule type

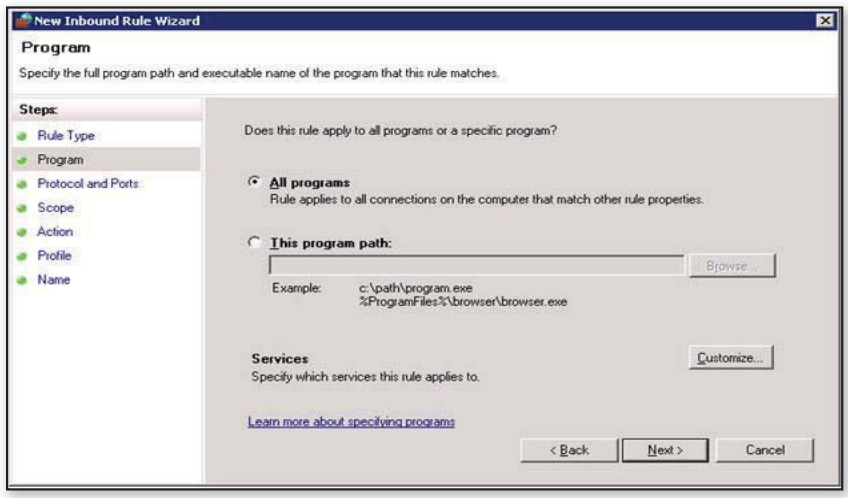


Figure 2: Specifying a program for a new inbound rule

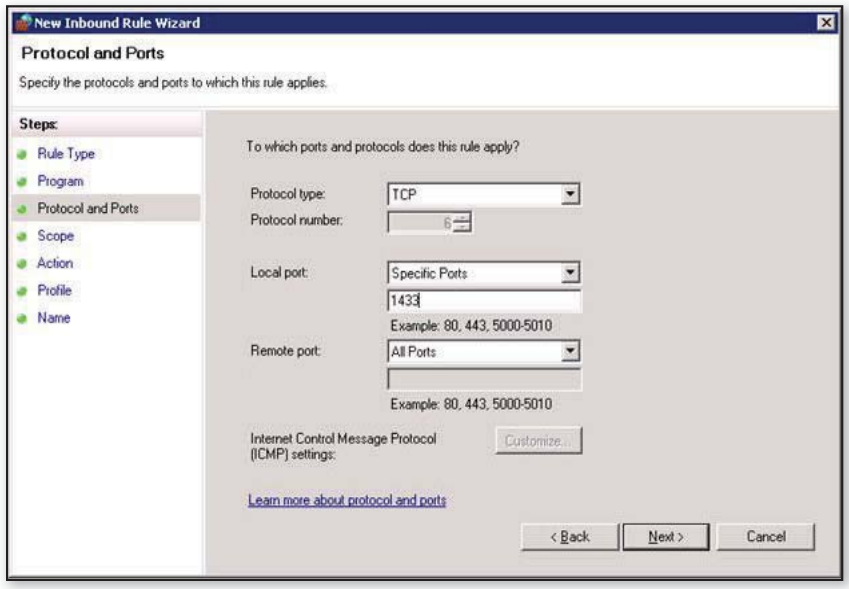


Figure 3: Specifying a protocol and ports for a new inbound rule

can be useful in an environment in which you have guests on the same network but you want to prevent them from accessing computers that are part of a domain. It can be used as an alternative or in addition to Virtual LANs (VLANs). For more information about domain isolation with IPsec tunnels, see the Microsoft TechNet article "Domain Isolation with Microsoft Windows Explained" at technet.microsoft.com/en-us/library/cc770610(WS.10).aspx.

Leave the Firewall Enabled

I suggest leaving the firewall enabled when Server 2008 R2 is first installed. Most applications are now smart enough to automatically open the necessary port on the firewall when they're installed, which eliminates the need to manually open inbound ports on the server. One of the main reasons to have the firewall up during installation is that it protects the OS before you have the chance to apply the latest updates.

The firewall is well-integrated with Server Manager's roles and features. When a role or feature is added on the server, the firewall automatically opens the necessary inbound ports. SQL Server uses the default port of TCP 1433. Therefore, you must manually create an inbound rule that allows TCP port 1433 on the firewall for SQL Server. (Alternatively, you can change the default.)

Creating Inbound Rules

If you leave the firewall enabled, you'll probably need to manually create an inbound firewall rule at some point. Fortunately, there are quite a few rules that are created but disabled by default for many popular Windows applications.

Before creating a rule, check to see whether a rule was already created that will allow the desired inbound traffic to pass. If you find an existing rule, you can simply enable the rule and possibly change the default scope. If you don't find an existing rule, you can always create one from scratch.

Select Administrative Tools from the Start menu, then select *Windows Firewall with Advanced Security* to start the *Firewall with Advanced Security* snap-in. For illustration purposes, I'll explain how to create a rule to allow inbound SQL Server traffic

on TCP port 1433 from a Microsoft Office SharePoint Server front-end server.

Right-click Inbound Rules and select New Rule. As Figure 1 shows, you can select Program, Port, Predefined, or Custom for the rule type. I typically select Custom, because this option prompts you to enter a scope for the rule. Click Next to continue.

In the next dialog box, which Figure 2 shows, you can specify a program or services that the rule will match. In my example, I selected *All programs* so that traffic will be controlled by the port number.

As Figure 3 shows, I then selected TCP for the protocol type, and I selected Specific Ports from the *Local port* drop-down menu and specified port 1433, which is the default port for SQL Server. Because remote ports are dynamic, I selected All Ports.

In the Scope dialog box, which Figure 4 shows, I specified the local IP address of 192.168.1.11 and the remote IP address of 192.168.1.10, which is the IP address of my organization's SharePoint front-end server. I strongly recommend specifying a scope with every rule, in case the server is accidentally exposed to unwanted subnets.

In the Action dialog box, which Figure 5 shows, I selected *Allow the connection* because I want to allow inbound traffic to pass for SQL Server. Alternatively, you can allow traffic to pass only if it's encrypted and secured with IPsec, or you can block the connection. Next, you need to specify the profile(s) for which the rule will apply. As Figure 6 shows, I selected all the profiles (which is a best practice). Finally, use a descriptive name for the rule, specifying the allowed service, scope, and ports, as Figure 7 shows. Using a descriptive name makes it easier to identify what a rule does. Click Finish to create the new inbound rule.

Creating Outbound Rules

By default, all inbound traffic is blocked and all outbound traffic is allowed on all three firewall profiles (i.e., domain, public, and private). If you use the default settings, you don't need to open any outbound ports. Alternatively, you can block outbound traffic—but then you must open up the necessary outbound ports.

Creating outbound rules is similar to creating inbound rules, except the traffic flow is reversed. You can use the *Firewall*

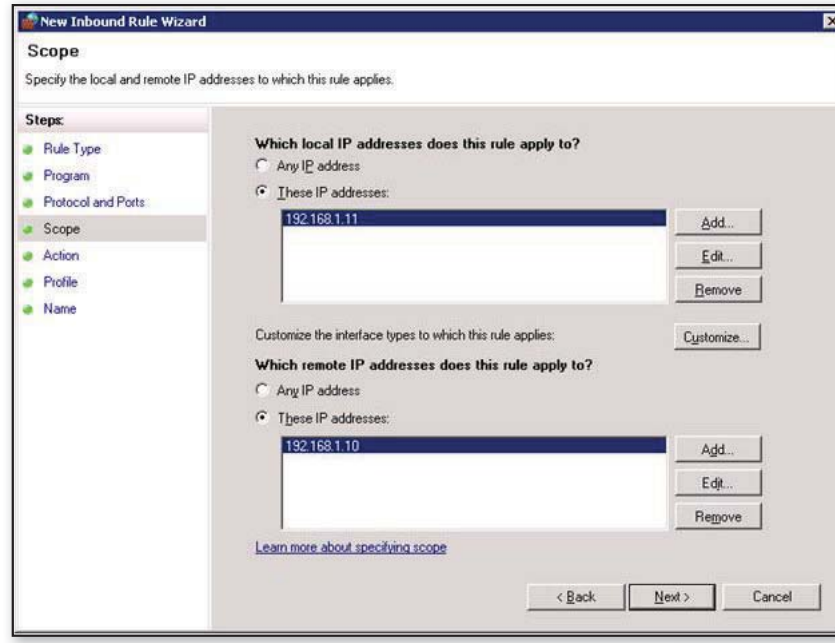


Figure 4: Specifying local and remote IP addresses in a new inbound rule's scope

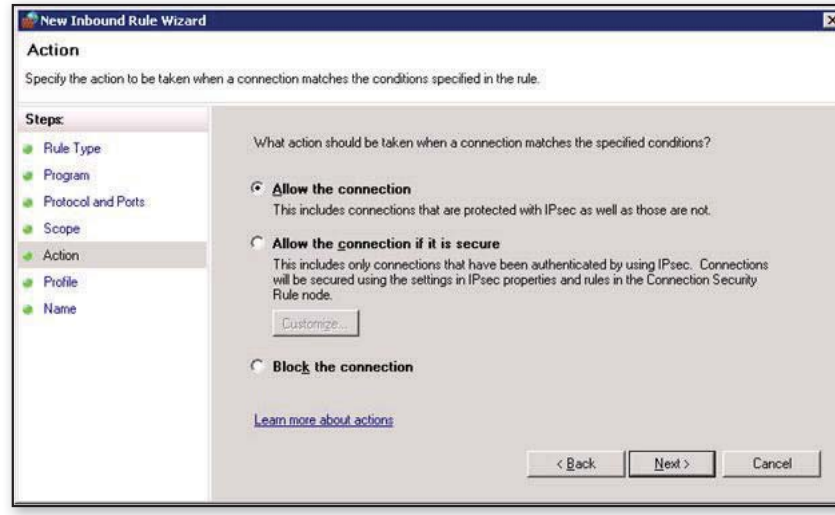


Figure 5: Specifying the action to take when a connection matches the condition in a new inbound rule

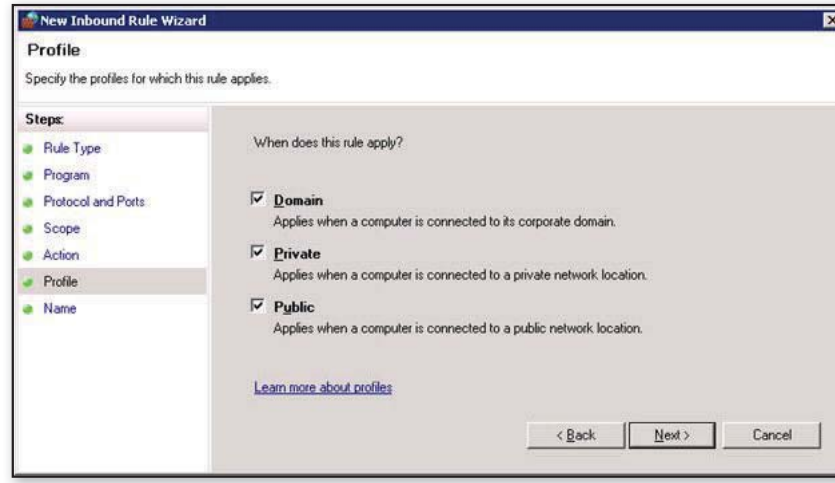


Figure 6: Specifying profiles for which a new inbound rule will apply

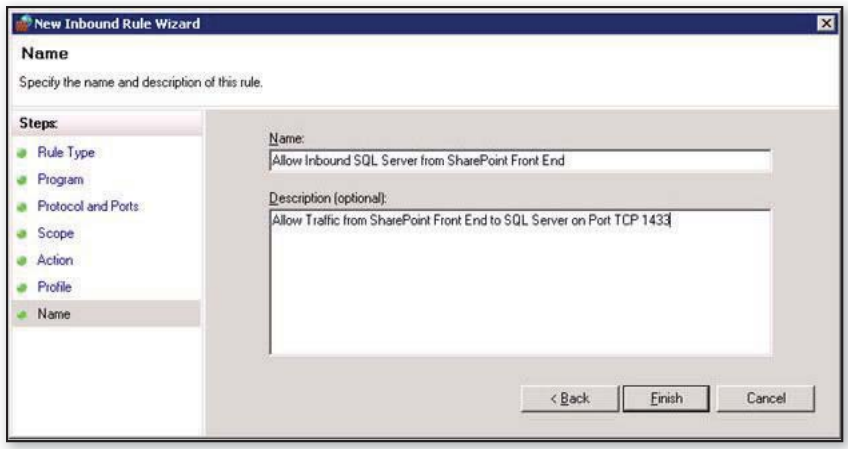


Figure 7: Naming a new inbound rule

with Advanced Security snap-in to block outbound traffic on specific ports if the server becomes infected with a virus and attempts to attack other computers on specific ports.

Managing Firewall Configuration

In addition to the *Firewall with Advanced Security* snap-in, you can use Netsh commands to create firewall rules. For more information about using Netsh to configure Windows Firewall, see the article "How to use the 'netsh advfirewall firewall' context instead of the 'netsh firewall' context to control Windows Firewall behavior in Windows Server 2008 and in Windows Vista" at support.microsoft.com/kb/947709.

You can also use Group Policy to control the configuration of the firewall. One of the easiest ways to push out a firewall rule with Group Policy is to use the *Firewall with Advanced Security* snap-in to create the rule, export it, and import it into the Group Policy Management Editor. Then you can use Group Policy to push out the rule to the appropriate computers. For more information about how to use Group Policy to control the Windows Firewall, see the article "Best Practice: How to manage Windows Firewall settings using Group Policy" at http://bit.ly/aZ4HaR.

Troubleshooting

If you're having difficulty connecting to a server that has Windows Firewall enabled, you can enable logging to determine if specific ports are being blocked. By default, firewall logging isn't enabled. To enable firewall logging, right-click *Windows Firewall with Advanced Security* and select Properties. Click the Active Profile tab (Domain, Private, or Public) under the Logging section, and click Customize.

> When trying to solve connectivity problems, I typically log only the dropped packets.

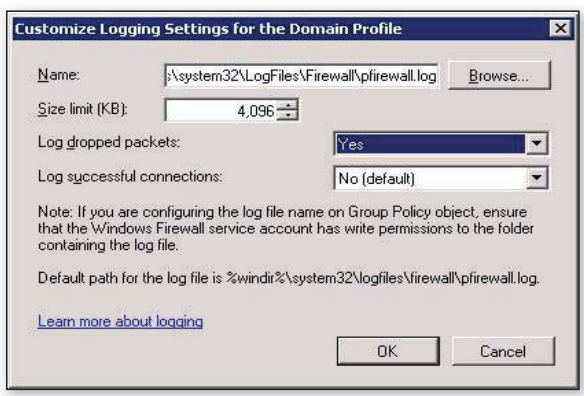


Figure 8: Enabling firewall logging for the domain profile

By default, the firewall log is located in C:\Windows\system32\LogFiles\Firewall\pfirewall.log. When troubleshooting connectivity problems, I typically log only the dropped packets, as Figure 8 shows; otherwise, the logs can fill up with a lot of successful connection information. Open the log with Notepad to determine if any packets are getting dropped by the firewall.

Another troubleshooting tip is to temporarily disable the firewall to see if doing so solves the connectivity problem. If you can establish a connection with the firewall disabled, open a command prompt and issue the command Netstat -AN to view the connection details. As long as the application is connecting with TCP, you can look at the local and foreign IP addresses with an *Established* state to determine the application's port(s). This can be especially helpful when you're not sure which port(s) a particular application uses to establish a connection.

The Windows Sysinternals tool TCPView, available at technet.microsoft.com/en-us/sysinternals/bb897437, is like Netstat on steroids. This tool provides detailed TCP connection information and can be helpful when troubleshooting connectivity issues.

Happy Firewalling

Server 2008 R2 and Server 2008 are the first versions of Windows Server that make it possible to keep the firewall enabled in a production environment. The trick is to leave the firewall enabled during installation of any programs on the server. This practice lets you test the server's connectivity before it goes into production. Use the *Log dropped packets* option to determine if any packets are getting dropped by the firewall. If you decide that you want to enable the firewall on the server after it's been in production for a while, I suggest that you establish a lab environment first to determine which ports are necessary to open on the firewall. Happy firewalling!

InstantDoc ID 140901



Alan Sugano
(asugano@adscon.com) is the president of ADS Consulting Group, which specializes in virtualization, networking, custom programming, Microsoft .NET web development, and SQL Server development. He's the author of *The Real-World Network Troubleshooting Manual* (Charles River Media).

FEATURE

Outlook 2010 Protection Rules

A useful complement to Exchange Server 2010's Transport Rules

by John Howie

In "Information Rights Management in Exchange 2010" (July 2010, InstantDoc ID 125022), I described some of the powerful new Information Rights Management (IRM) features in Microsoft Exchange Server 2010, including the use of Transport Rules to automatically apply rights protection to email messages and the ability to consume rights-protected email messages in Outlook Web Access (OWA), making it easier to protect your company's most sensitive information as it flows through email. In this article, I describe the new features in Microsoft Outlook 2010 that you can use to further expand data protection, and I explain how to configure your servers and end user systems to take advantage of these features.

Creating Outlook Protection Rules

Although Exchange 2010 has powerful IRM features, there's always the concern that a user might send a sensitive email message that's unprotected (e.g., over a public network) until it reaches your Exchange 2010 server and is detected and processed by a Transport Rule. In large organizations, where many sensitive email messages are sent, you might not want to rely on the use of Transport Rules because heavy use can affect performance.

Transport Rules have numerous potential performance problems, ranging from rules that require in-depth analysis of email and attachments, to the actions that must be performed when a rule fires (such as encrypting a message and attachments). The performance effect depends on the type of rules, the actions that must be performed, and how often they fire (typically tied to mail volume).

Depending on compliance obligations, your company might need to encrypt certain types of data, including email messages with information about customers, before transmitting it from a desktop or laptop. In addition, you might not have Exchange 2010 fully deployed yet, meaning you can't take advantage of IRM features in Exchange 2010 Transport Rules. For all these reasons, you should consider using the new IRM feature in Outlook 2010 called *Outlook protection rules*.

Outlook protection rules aren't as sophisticated as Transport Rules and are limited to applying rights protection to email messages based on one or more of the following three criteria: the department or group the sender of the email message is in; the recipient email address; and the scope of the email message (whether the recipients are inside or outside the organization). The protection rules are created on your Exchange 2010 servers using PowerShell scripts. You need Exchange 2010 deployed sufficiently so that rules can be distributed to Outlook 2010 by using Exchange web services.

Outlook protection rules are based on rights policy templates. You need to create these templates on your Active Directory Rights Management Services (AD RMS) servers. If you already have existing templates that will apply the policies you need, you can reuse them. You can enumerate the list of templates available from the Exchange Management Shell (EMS) using the command Get-RMSTemplate. The list returned will always contain the default template named Do Not Forward. You need to be careful, though, when creating or using existing templates because it's possible to create an Outlook protection rule that specifies a particular template be used with a set of users and rights that will render

rights-protected email messages unreadable by recipients or might allow recipients to forward the email messages or even print them. Always check the rights specified in a template before using it.

You might find it simpler to create new templates that specify Anyone as a consumer of rights-protected content, rather than specific named users, and ensure that the right to forward an email message isn't selected in those templates. This configuration will ensure that all users can read an email message they receive that was rights protected by an Outlook protection rule but can't forward the email message to anyone else.

After your rights policy templates are set up, you create Outlook protection rules using the New-OutlookProtectionRule cmdlet in the EMS. You can't create Outlook protection rules using the Exchange Management Console (EMC) or Exchange Control Panel (ECP). There are only two required parameters to the cmdlet. The first is the name of the Outlook protection rule and is specified by the argument -Name <*rule name*>. You'll use the rule name to manage the Outlook protection rule. The second required parameter is the name of the rights policy template and is specified by the argument -ApplyRightsProtection Template <*rights policy template*>. In addition to specifying the rule name and rights policy template to be applied, you need to specify the conditions under which the rule will be applied.

To specify that a rule is applied when the sender is from a particular department, use the -FromDepartment <*department name*> argument, where <*department name*> is one or more departments that the rule should apply to. The argument <*department name*> is checked against the department attribute on the user object corresponding to the user sending the email message to see if a match exists and whether or not the rule should apply. You can set users' departments by editing the Department field on the Organization tab of one or more users' Properties dialog box, which can be viewed in the EMC or in the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.

To apply a rule based on the recipient, use the -SentTo <*recipient name*> argument. The <*recipient name*> parameter can be the names of one or more recipients in Outlook's address book and can be one or more SMTP addresses (which are typically used for external recipients). Note that if you create a rule that specifies a distribution or mail-enabled security group, the rule won't apply when an email message is sent to one or more members of the group without using the group name. The rule will apply only when the group name specified in the rule matches a recipient on the To:, Cc:, or Bcc: lines in Outlook.

The condition you can specify is the scope of recipients, using -SentToScope <*scope*>. The two possible values for <*scope*> include InOrganization and All. InOrganization specifies that the rule applies when the recipients are internal to the organization; All specifies that the rule applies regardless of who the recipient is. Although this rule can be used on its own, it's typically used as a modifier to either or both of the previous two rules.

If you create many Outlook protection rules, you might end up with two or more rules that apply based on the department the sender is in, the intended recipient(s) of the email message, and the scope of the recipient(s). You can control the order in which rules apply by using the argument -Priority <*n*>, where *n* is a number. The default priority is 0. Rules with lower priorities are checked first. When a rule match is found, the specified template is applied, and processing stops. When a rule is matched and a template is applied, the user can choose to override the Outlook protection rule. To prevent a user from overriding a rule, and to force a template to be applied, you can supply the argument -UserCanOverride $false.

The following command creates an Outlook protection rule that applies the rights policy template FTE Only to all email messages sent to the distribution group InfoSec Research FTE and that can be overridden by the sender:

```
New-OutlookProtectionRule -Name
    "InfoSec Research FTE - FTE Only" '
 -ApplyRightsProtectionTemplate
    "FTE Only" '
 -SentTo "InfoSec Research FTE"
```

You can enumerate the Outlook protection rules on your systems from the EMS with the cmdlet Get-OutlookProtectionRule. Rules can be enabled and disabled by using the cmdlets Enable-OutlookProtectionRule and Disable-OutlookProtectionRule and can be deleted with the cmdlet Remove-OutlookProtectionRule. All four cmdlets let you specify the rule with the argument -Identity <*rule name*>. Finally, a rule can be modified using Set-OutlookProtectionRule, specifying the rule to modify using the -Identity parameter. The other parameters accepted by this cmdlet are identical to those used in New-OutlookProtectionRule.

Configuring End Users' Systems

Before templates specified in Outlook protection rules can be applied to email messages, the rights policy templates specified must be available to Outlook. The built-in template Do No Forward is always available, and any Outlook protection rules that use that template will work without any configuration of end users' systems.

Rights policy templates are XML files; it's common to configure AD RMS to store them on a central file share and to configure Microsoft Office applications to point to the file share so that these templates are available to users. An alternative is to copy the templates to users' machines and configure Office applications to access them on a local drive.

Prior to Windows Vista, distributing rights policy templates meant periodically running a custom script or application to copy templates from a central share. However, in Vista and later, as well as in Windows Server 2008 and later, built-in Task Scheduler templates work with AD RMS to download rights policy templates, as Figure 1 shows.

The first template is intended to be used by domain-joined end user systems; it runs at a preset time (3:00 A.M.) and when a user logs on. The second template is intended to be used on systems that aren't domain joined; it requires you to override the EnterprisePublishing registry entry used by non–domain-joined AD RMS clients.

Each task checks to see whether the user has obtained templates in the past 30 days or more. If so, the task contacts the AD RMS infrastructure to obtain rights policy templates. It can take as long as an hour after a user logs on to a system for the scheduled task to run, as well as to copy templates,

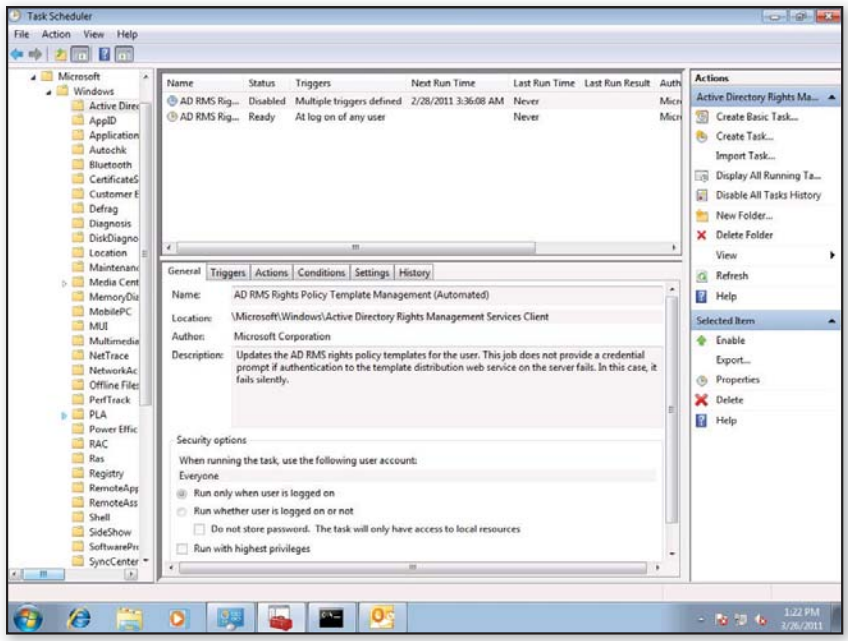


Figure 1: Automatically updating AD RMS rights policy templates

if required. The templates are stored in the folder \%LocalAppData%\Microsoft\DRM\Templates. The folder \%LocalAppData% is mapped to the folder \AppData\Local in each user's profile folder, which is typically C:\Users\<*username*>. If you change templates frequently and need the tasks to fetch templates more often than every 30 days, you can create a DWORD registry entry called UpdateFrequency under the HKEY_CURRENT_USER\Software\Microsoft\MSDRM\TemplateManagement registry entry. The value of the registry entry is the number of days that should elapse before checking for new, changed, or deleted templates.

Configuring the Task Scheduler on each end user's machine to download rights policy templates probably isn't feasible for your organization if you have several end user systems. Instead, you can use an alternative method, such as a network share configured as an offline folder on the client. Another alternative is to run a logon script to copy templates, as you probably did pre-Vista.

Regardless of how you distribute templates to end users' systems, you need to set a per-user registry entry to configure Microsoft Office 2010 to find the templates. This registry entry is HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\DRM for 32-bit editions of Office 2010 running on 32-bit editions of Windows and 64-bit editions of Office 2010 running on 64-bit editions of Windows. For 32-bit editions of Office 2010 running on 64-bit editions of Windows (which is the default when installing Office 2010 on a 64-bit edition of Windows), the registry entry is HKEY_CURRENT_USER\Software\Wow6432Node\Microsoft\Office\14.0\Common\DRM. The registry entry is AdminTemplatePath, and the entry type is Expandable String Value.

You don't need to visit each of your end users' systems to configure the correct registry entry if you download and install the Office 2010 Administrative Template files and Office Customization Tool, available from www.microsoft.com/download/en/details.aspx?&id=18968. The download includes various templates that can be used to create Group Policy Objects (GPOs) that can control many aspects of Office 2010, including where it searches for rights policy templates. Make sure you download the correct pack—there are packs for the 32-bit and 64-bit editions of Office 2010.

To configure the AdminTemplatePath setting for your end users by using a Group Policy setting, download and install the administrative templates (under the ADMX folder) to C:\Windows\PolicyDefinitions or to the Group Policy central store. Alternatively, you can manually add the file office14.adm template to the Group Policy Management Editor. Create a new GPO, open it for editing, and navigate to \User Configuration\Policies\Administrative Templates\Microsoft Office 2010 (there's a node for legacy administrative templates above the last node if you use the ADM file). Select the node Manage Restricted Permissions, then double-click Specify Permission Policy Path in the right-hand pane. In the Specify Permission Policy Path dialog box, select Enabled and enter the path to the rights policy templates, as Figure 2 shows.

If you're using Offline Folders, this folder will be shared. If you're copying files to end users' machines, the templates will be stored in this folder. After the GPO is created, link it to an organizational unit (OU) that your users are in.

A large gotcha when using GPOs to set the AdminTemplatePath setting for use by Office applications is that the registry entry is fixed as a REG_SZ type, which means you can't use a variable such as

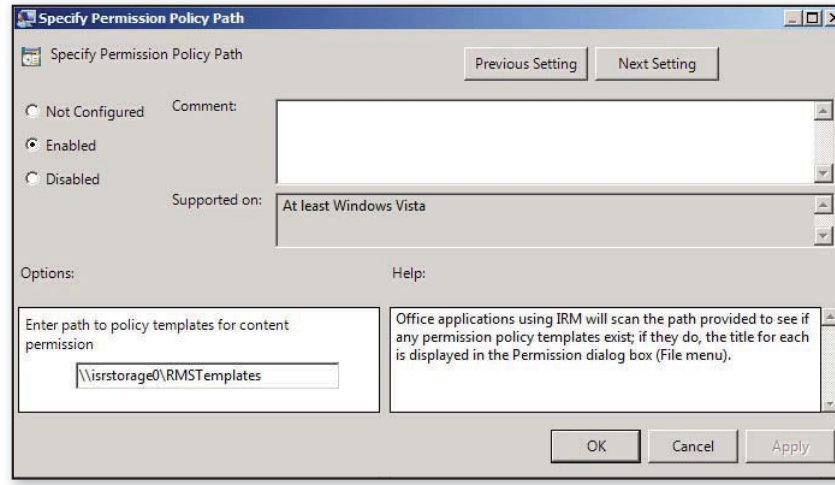


Figure 2: Specifying a path for policy permissions

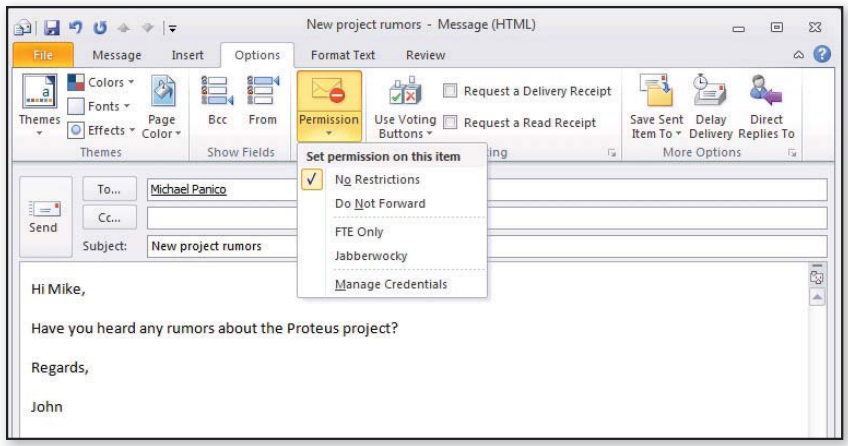


Figure 3: Checking template availability

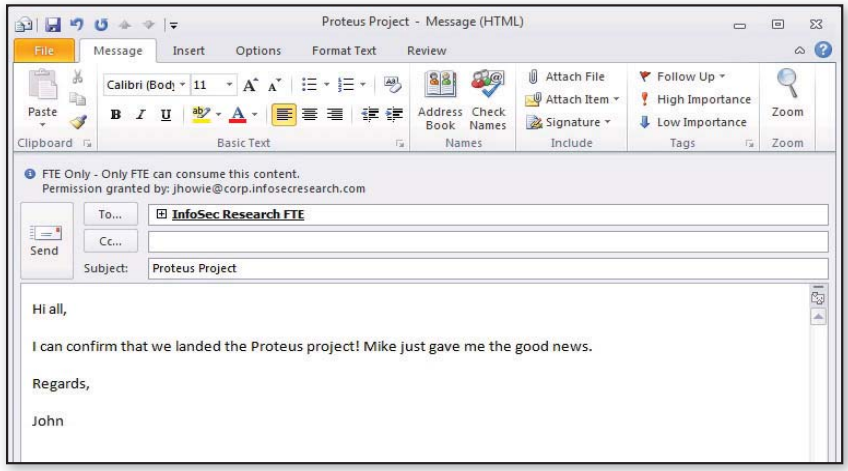


Figure 4: Notification of Outlook protection rule application

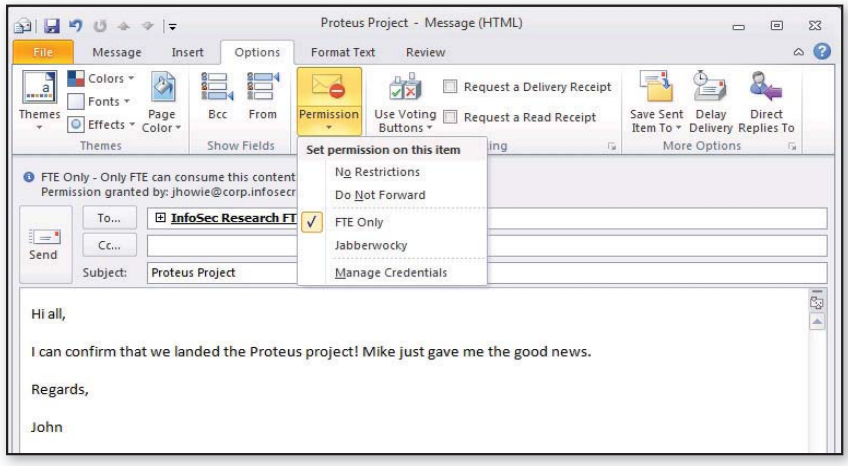


Figure 5: Checkmark indicating applied rights policy template

%LocalAppData% when specifying the location of the rights policy templates—which pretty much precludes using a GPO to point to the Templates folder populated by the Task Scheduler. For this reason, I recommend setting AdminTemplatePath to the file share where RMS templates are stored and configuring administratively assigned offline files (under \User Configuration\Policies\Administrative Templates\Network\Offline Files) to add the location of the share where the templates are stored in the same GPO. This configuration ensures that the most recent templates are available to end users (without waiting for the Task Scheduler to pick them up) and available offline for laptop users when they disconnect from the network.

You can test the availability of templates to Outlook 2010 by logging on as a user who has AdminTemplatePath GPO settings, creating a new email message, and selecting the Permission drop-down on the Options tab, as Figure 3 shows. If templates are available, they're listed between Do Not Forward and Manage Credentials.

End User Experience

The end user experience with Outlook protection rules is seamless. When an email message matches one of the Outlook protection rules' specified conditions, the appropriate rights policy template is applied to the email message and a visual cue is presented, as Figure 4 shows. Unless the rule specifies that the user can't override the rights policy template, the user can select the Permission drop-down on the message's Options tab and select No Restrictions. (The rights policy template that was applied to the message will have a checkmark next to it, as Figure 5 shows.)

One thing Outlook protection rules can't do is prevent end users from sending sensitive email messages without protection when using a browser, OWA, or a mobile device. You should therefore consider using Outlook protection rules with Exchange 2010 Transport Rules to create a complementary IRM strategy. You can also prevent users with desktops and laptops from using OWA to send email messages, to ensure that Outlook protection rules aren't bypassed.

Extend Your Protection

Outlook protection rules let you extend protection of sensitive information to the desktop and can help you meet compliance obligations. They complement Exchange 2010's Transport Rules, and they can be used to do away with the need for some Transport Rules, which helps offload processing from your Exchange 2010 infrastructure.

InstantDoc ID 139816



John Howie
(jhowie@microsoft.com) is a senior director in the Online Services Security & Compliance team at Microsoft, where he manages cloud security.

GREAT WEB HOSTING
THE BEST VALUE
FOR YOUR BUSINESS

✓ **Superior Website Security with 1&1 Dual Hosting:**
Your website is simultaneously hosted in 2 locations in our geo-redundant data centers!

✓ **Unlimited Access**
65 Click & Build Applications.

✓ **Unlimited Support**
24/7 Technical Support.



	1&1	GoDaddy®	Network Solutions®
Package	Unlimited	Deluxe	Large
Web Space	unlimited	150 GB	500 GB
Traffic	unlimited	unlimited	unlimited
Domains	1 FREE	$11.99 (per year)	1 FREE
Private Domain Registration	FREE!	$9.99 (per year)	$9.99 (per year)
1&1 Dual Hosting	✓	–	–
Monthly Cost	$3.49*	$6.79	$13.29
Annual Cost (incl. domain)	$ 41.88 first year, then $83.88	$103.46	$169.97

YOUR PRIVACY IS IMPORTANT. WE AGREE.

That's why at 1&1, all domains come with FREE Private Domain Registration to protect your name, address, phone number and e-mail from spammers and identity thieves.

MEMBER OF united internet

1-877-461-2631 www.1and1.com
1-855-221-2631 www.1and1.ca

1&1®

* $3.49/month offer valid with 12 month minimum contract term only. Upfront payment due upon sign up. Setup fee and other terms and conditions may apply. Private domain registration is available for .com, .net, .org, .info, .biz, .tv, .mobi, .name, .ws, and .cc domains. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet, all other trademarks are the property of their respective owners. © 2011 1&1 Internet. All rights reserved.

Windows IT Pro Congratulates **Cisco**



Category: **Hardware: Networking**
Product: **Cisco Catalyst 6500 Series**
Award: **Community Choice Gold**



Category: **Hardware: Server**
Product: **Cisco Unified Computing System**
Award: **Community Choice Bronze**

Learn more about Cisco here: www.cisco.com/go/microsoft

we're not just making servers. we're making server history.

©2011 Cisco Systems, Inc. All rights reserved. All third-party products belong to the companies that own them.

While innovation comes rapidly in the IT industry, basic server architectures haven't changed for decades. That's why Cisco answered the need for innovation by introducing the Cisco Unified Computing System – which integrates compute, high-speed networking, storage access and virtualization in one system. Since its introduction, IT departments have dramatically reduced data center complexity while:

- Lowering operating costs by up to 30%
- Reducing Microsoft deployment times from weeks to minutes
- Harnessing the power of the UCS architecture for Microsoft Window Server and Exchange, SharePoint, and SQL Server deployments

The Cisco Unified Computing System, powered by intelligent Intel® Xeon® processors, signals the next evolution of the data center – where everything, and everyone, works together like never before.

Find out more at www.cisco.com/go/microsoft

together we are the human network. cisco



FEATURE

Easily find Special Folder Paths with PowerShell

Paths to key OS and user folders aren't always standardized

by Alex K. Angelopoulos

Even in the most standardized networks, it's easy to specify the incorrect paths to special folders such as My Documents or temporary folders that have special roles in Windows. Fortunately, you can ask Windows where particular folders are located. After I explain the root of the problem, I'll show you how to make Microsoft PowerShell scripts consistently find the correct path, even in nonstandard setups.

Understanding the Problem

Although working with files and folders is a standard task for network administrators, the specific paths to those folders aren't standard. Windows installations, upgrades, hardware installations, user policies, and machine policies can all lead to wildly varying paths for special folders. Even in standardized networks, variations are possible due to machine roles or user requirements. Some of these paths are relatively easy to find with PowerShell variables. For example, the $home variable always contains the literal path to a user's home folder. However, finding other paths might require some guesswork. For example, if your users are mainly running Windows 7 or Windows Vista, you could try accessing the folder that contains temporary Internet files by using the path \$home\AppData\Local\Microsoft\Windows\Temporary Internet Files. However, this path will fail for users running an earlier Windows OS or if their temporary Internet files are redirected to a different location.

Standardizing isn't always possible, and coding in checks for special cases is cumbersome and confusing. Instead, you can use the Microsoft .NET Framework's System.Environment class to obtain paths. By using the OS APIs, you have access to more information than you can get from environment variables alone. The information is also more reliable because Windows uses the same technique to determine paths.

Using System.Environment in PowerShell

In PowerShell, you specify a .NET class by using its name in square brackets, like this: [System.Environment]. To simplify using the System namespace, PowerShell lets you omit the *System.* portion, so you can use [Environment] for brevity. To find the paths of special folders, the first step is to determine what special folders are exposed. The Environment class has a special enumerated list of the canonical names for these folders. A quick way to show these names is to use the command

```
[Environment+SpecialFolder]::GetNames([Environment+SpecialFolder])
```

In Windows 7, this command returns a list of names like that shown in Web Figure 1 (www.windowsitpro.com, InstantDoc ID 140658). You can find the meanings of these names in the "Environment.SpecialFolder Enumeration" web page (msdn.microsoft.com/en-us/library/system.environment.specialfolder.aspx). Note that some of the special folders listed in this web page aren't available within PowerShell.

At the bottom of the "Environment.SpecialFolder Enumeration" web page, you'll find a PowerShell script by Thomas Lee demonstrating how to list the special folders' names and their paths. There

Listing 1: Code to Create a Hash Table That Contains Special Folders' Names and Paths

```
$SpecialFolders = @{}
$names = [Environment+SpecialFolder]::GetNames( `
  [Environment+SpecialFolder])
foreach($name in $names)
{
  if($path = [Environment]::GetFolderPath($name)){
    $SpecialFolders[$name] = $path
  }
}
```

Listing 2: Code to Create Named Drives from Special Folders' Paths

```
$names = [Environment+SpecialFolder]::GetNames( `
  [Environment+SpecialFolder])
foreach($name in $names)
{
  if($path = [Environment]::GetFolderPath($name)){
   New-PSDrive -Name $name -PSProvider FileSystem -Root $path
  }
}
```

Listing 3: Code to Find the 10 Largest Files in the Documents Folder

```
gci Personal: -Recurse -Force -ea SilentlyContinue |
  Sort-Object -Property Length -Descending |
  Select-Object -First 10 |
  Format-Table -AutoSize -Wrap -Property `
    Length,LastWriteTime,FullName
```

Listing 4: Code to Display the Name and URL for Each Favorite Item in IE

```
gci -Path Favorites:\ -Recurse |
  ?{$_.Length} |
  %{$_.BaseName; Get-Content $_.FullName |
  Select-String ^url=*|
  %{$_ -replace "^url="," ";""}
}
```

are two details you should know about accessing these folders. First, if a folder doesn't exist, you'll get an empty path back. Second, some folders might not be accessible from an unprivileged account.

Thomas Lee's script works well if you just want to see the names and paths. However, what can you do if you want to easily use those paths in scripts? There are many possible approaches. I'll show you three of them. Each is useful in different situations, but all of them require that you understand what the names like ProgramFiles or Startup mean, as defined in the "Environment.SpecialFolder Enumeration" web page.

Suppose you want to access a specific folder, such as the one named Desktop. In PowerShell syntax, the ID of this specific folder is [Environment+SpecialFolder]::Desktop. You provide this ID as an argument to the Environment class's static GetFolderPath method, like this

```
[Environment]::GetFolderPath("Desktop")
```

This command returns the exact path to the current user's Desktop folder.

To get an entire list of folders and their paths (which are accessible by name), you can use the code in Listing 1. It creates a hash table named $SpecialFolders, gets the names of all the special folders known to the .NET Framework, then gets the paths of those folders. The code adds each non-empty special folder path to the hash table, indexed by the folder name. You can see the contents of the hash table by simply entering $SpecialFolders after the PowerShell prompt and pressing Enter. Web Figure 2 shows sample results from running the code in Listing 1.

Turning Special Folders Into Drives

I like to create PowerShell drives from each special folder path, using the canonical folder name as the drive name. The code in Listing 2 creates named drives from the special folder paths, producing output similar to Web Figure 3, depending on your system. It's then possible to access items using these drive names without having to think about user context or actual paths. You can see the drives' actual paths by running the code

```
Get-PSDrive | ft name,root -AutoSize
```

When you need to perform tasks in a special folder, you just need to specify the drive name. For example, to copy the entire set of Favorites items in Internet Explorer (IE) to a folder on the F drive, run the command

```
Copy-Item -Path Favorites:\ `
  -Destination F:\Favorites -Recurse
```

To list the last 20 documents accessed in reverse chronological order, use

```
gci Recent: | Sort-Object -Property `
  LastWriteTime -Descending
```

The code in Listing 3 finds the largest 10 files in the Documents folder and shows them in descending order based on size. The output includes the last time the files were modified (LastWriteTime) so that you can determine if any of the files are currently being edited. The code in Listing 4 retrieves the display name and URL for each Favorite item in IE, generating a scrollable list with spaces between items for easy reading.

Considering Other Methods

Using System.Environment is the most reliable way to find a path to a special folder. Creating PowerShell drives from these paths makes this technique very useful. But sometimes you can't find what you need this way. Alternatively, you can construct a path using standard PowerShell variables (or shell variables accessible through the env: drive) and some guesswork—although this technique is less reliable. You should at least use PowerShell's Test-Path cmdlet to confirm that the path exists. Another technique is to use the Shell.Application COM object's NameSpace method. You can also use this method in Windows Script Host (WSH) scripts. To explore this technique, search the Internet using Shell.Application and NameSpace as the search terms. My preferred method is to create PowerShell drives with the code in Listing 2. It lets me concentrate on the task instead of the mechanics for performing it.

InstantDoc ID 140658



Alex K. Angelopoulos (aka@mvps.org) is an IT consultant, an MCSE, and a contributing editor for *Windows IT Pro*. As an avid scripter, he regularly writes about administrative automation using WSH, PowerShell, and related technologies.

WE KNOW YOUR INDUSTRY.

AGRICULTURE

AUTOMOTIVE & TRUCKING

BROADCAST ENGINEERING

AVIATION

COMMERCIAL REAL ESTATE

DESIGN ENGINEERING

ELECTRONICS

ELECTRICAL SYSTEMS, ENERGY & CONSTRUCTION

FOOD

HEALTHY LIFESTYLE

IT & DEVELOPER

MANUFACTURING & SUPPLY CHAIN

MARKETING & MEETINGS

MECHANICAL SYSTEMS

PUBLIC INFRASTRUCTURE

RESTAURANTS

WEALTH MANAGEMENT

WE KNOW YOUR CUSTOMERS.

WHAT THEY'RE READING. WHAT THEY'RE SEARCHING FOR. WHAT THEY'RE DOWNLOADING.

WE KNOW HOW TO CREATE AND DELIVER CONTENT THAT PERFORMS.

WHITE PAPERS

WEBINARS

CONFERENCES

SEARCH MARKETING

SOCIAL MEDIA

LEAD NURTURING

VIDEOS

WEBSITES

RESEARCH

Penton Marketing Services
WE KNOW YOUR CUSTOMERS
powered by eyetraffic

Windows IT Pro

CONTACT:
Chrissy Ferraro
970-204-0952
PentonMarketingServices.com

Wi-Fi Best Practices

Enhance your security, reliability, and availability

by Michael Dragone

Like most technologies that an IT pro deals with, wireless technology changes from day to day. Not too long ago, having a wireless LAN (WLAN) was considered a mere luxury or something "nice to have." Nowadays, however, access to a WLAN is critical because the proliferation of mobile devices that have entered our industry invariably tout Wi-Fi as a key selling point. This is even more important as cellular carriers begin to cap their wireless data rate plans; unlimited cellular data plans are all but gone, whereas Wi-Fi is almost always unlimited (and faster).

It's important to take stock of your current WLAN infrastructure if you have one, and to be aware of the latest standards if you're designing a new one—even if it consists of only a single Access Point (AP). In this article, I take a look at the current wireless standards and discuss some common-sense best practices related to radio spectrum bands, channel selection, and security that you can begin implementing today to enhance the security, reliability, and availability of your Wi-Fi setup.

The Band Played On

Almost all discussions of Wi-Fi include at least a mention of spectrum bands—and our discussion is no different. In the United States, there are two spectrum bands commonly associated with Wi-Fi: the 2.4GHz band and the 5GHz band. Both are part of a broader set of radio bands known internationally as the industrial, scientific, and medical (ISM) bands. In general, access to all of these radio bands is unrestricted, subject to local regulations. This is great for saving on FCC licensing costs, but it comes at the expense of having to share these radio bands with a potential smorgasbord of other devices.

The IEEE standard that governs WLANs is called specification 802.11. IEEE standards specify the protocols that define the frequency, bandwidth, maximum data rates, and modulation of wireless signals. We're concerned with the primary four: 802.11a, 802.11b, 802.11g, and 802.11n—leaving legacy 802.11 (i.e., 802.11-1997) by the wayside.

802.11b is perhaps the most well-known protocol, and for good reason. It was the first protocol to gain widespread acceptance in the industry; the majority of the subsequent protocols are backward-compatible with it. Originating in 1999, 802.11b operates at 2.4GHz, with a maximum throughput of 11Mbps.

802.11a also originated in 1999, as a speedier alternative to 802.11b. This was achieved by having 802.11a operate in the 5GHz band with Orthogonal Frequency Division Multiplexing (OFDM) modulation. Compared with the Direct Sequence Spread Spectrum (DSSS) modulation used by 802.11b, this allows 802.11a devices to achieve a maximum throughput of 54Mbps. The primary drawback to 802.11a is the lack of compatibility with 802.11b.

802.11g came on the scene in 2003, combining the best of 802.11b and 802.11a. 802.11g operates in the 2.4GHz band and is backward-compatible with 802.11b devices by supporting both DSSS and

OFDM modulation. This allows 802.11g devices to achieve a maximum throughput of 54Mbps, with one caveat: Adding a single 802.11b device to an 802.11g network drops the maximum throughput of the network back to the 11Mbps 802.11b level.

802.11n is the newest and currently favored protocol. Arriving in 2009, 802.11n greatly enhances wireless networking by supporting a maximum throughput of 600Mbps. However, achieving this radical speed isn't a given. 802.11n works in both the 2.4GHz and 5GHz bands, using OFDM modulation. In the 2.4GHz band, 802.11n supports up to four multi-input multi-output (MIMO) streams (radio channels) across 20MHz of bandwidth for a maximum throughput of 260Mbps. In the 5GHz band, 802.11n likewise supports four MIMO streams but combined with a higher maximum bandwidth of 40MHz allows for a maximum 600Mbps throughput. 802.11n includes backward-compatibility for not only 802.11g and 802.11b but also for 802.11a.

Before we move on to radio channels, a quick discussion of the 2.4GHz radio band versus the 5GHz band is in order. The 2.4GHz band is more crowded because it has to share spectrum with plenty of other unlicensed devices. Microwave ovens, baby monitors, and cordless phones compete in this band for available spectrum. Similarly, the number of usable radio channels in the 2.4GHz band is more limited. The 5GHz band is less crowded and has more usable channels, at the expense of a slightly shorter maximum range.

Channel Surfing

Within the 2.4GHz and 5GHz radio bands, there are numerous channels that a Wi-Fi device can use. Although a complete discussion of radio signal modulation, channel subcarriers, channel separation, and other geeky topics is beyond the scope of this article, there are some basic ideas about Wi-Fi radio channels you should be familiar with.

In the United States, at 2.4GHz, there are 11 channels to choose from. However, the exact frequencies of these channels overlap slightly as you increment from 1 through 11. This reduces the number of non-overlapping channels greatly, specific to the 802.11 protocol and channel width in use. Avoiding the overlapping channels allows for greater range and throughput of your wireless networks.

- For 802.11b, channels 1, 6, and 11 won't overlap.
- For 802.11g and 802.11n with a 20MHz channel width, channels 1, 5, and 9 won't overlap.
- For 802.11n with a 40MHz channel width, channels 3 and 11 won't overlap.

At 5GHz (again in the United States), things are much easier. For 802.11a and 802.11n with either a 20MHz or 40MHz channel width, channels 36, 40, 44, 48, 149, 153, 157, 161, and 165 are available and won't overlap with each other. Channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 136, and 140 are also available without overlap as long as the Wi-Fi equipment supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) capabilities.

Avoiding the overlapping channels allows for greater range and throughput of your wireless networks.

This is because of an FCC rule designed to protect other equipment, primarily military and weather-related, that uses those channels. If your Wi-Fi AP doesn't support DFS and TPC, those channels shouldn't even be available to you for selection.

Security, Not Obscurity

We've discussed bands and channels—now, what about security? Every AP on the market supports at least some type of Wi-Fi encryption, but if you fire up your Mac or PC and scan the radio waves for nearby WLANs, you'll likely see many networks with weak encryption, or even none at all.

Wired Equivalent Privacy (WEP) is the oldest encryption algorithm available for use and one you should completely avoid. In addition to 64-bit encryption, WEP supports 128-bit encryption—but don't let the higher number fool you. Both have numerous security flaws, and it's trivial to defeat the encryption on a WLAN using WEP. There are even downloadable utilities that can be installed that will do the decrypting for you in a matter of minutes. WEP has been completely deprecated and shouldn't be used.

Wi-Fi Protected Access (WPA) was designed to replace WEP and its associated weaknesses. WPA was found to have some security weaknesses, but it's nowhere near as weak as the flaws found in WEP. Further development led to the more secure Wi-Fi Protected Access 2 (WPA2), the current gold standard in Wi-Fi security.

WPA and WPA2 are available in two modes: Personal (or pre-shared key—PSK) mode and Enterprise (or 802.1x) mode. Personal mode (i.e., WPA-PSK) is designed for small office/home office (SOHO) users, allowing easy setup with a predefined key entered on an AP and subsequent Wi-Fi clients. Enterprise mode (i.e., WPA-Enterprise) uses a Remote Authentication Dial-In User Service (RADIUS) server and the Extensible Authentication Protocol (EAP) to authenticate users or Wi-Fi devices before allowing access to a dynamically changing encryption key used by the AP. (For information about Enterprise mode, see "A Secure Wireless Network Is Possible," www.windowsitpro.com, InstantDoc ID 42273.)

WPA and WPA2 also support two encryption protocols: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). TKIP is used by WPA. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is used by WPA2; because CCMP is based on AES, CCMP is typically referred to simply as AES. In Personal mode, you'll typically see these encryption options referred to in documentation and AP management software as WPA-PSK (TKIP) or WPA2-PSK (AES).

Putting It All Together

I've given you a lot of information—but how do you put it to good practical use? Clearly, 802.11n is the preferred choice for new WLAN installations and upgrades. But how can you achieve the maximum 600Mbps throughput? What about selecting between 2.4GHz and 5GHz and dealing with devices that don't support WPA2-PSK (AES)? To

Learning Path

Windows IT Pro Resources

"Wi-Fi Alliance: Please Set Wireless Networks to WPA2," InstantDoc ID 136743

"Enabling 802.11i Wireless Security with Windows Servers," InstantDoc ID 98796

"Easy 802.11g Security," InstantDoc ID 48168

"Secure Your Wireless Network," InstantDoc ID 47860

"A Secure Wireless Network Is Possible," InstantDoc ID 42273

"Planning for Wi-Fi," InstantDoc ID 39528

Microsoft Resources

"802.1x Authenticated Wireless Deployment Guide," technet.microsoft.com/en-us/library/dd283093(WS.10).aspx

"Wireless Networking Security," technet.microsoft.com/en-us/library/bb457019.aspx

"Secure Wireless Access Point Configuration," technet.microsoft.com/en-us/library/cc875845.aspx

"5-Minute Security Advisor - Strengthening Wireless Authentication," technet.microsoft.com/en-us/library/cc722665.aspx

"Wi-Fi: 8 tips for working securely from wireless hot spots," www.microsoft.com/atwork/remotely/hotspots.aspx

answer these questions, I came up with the following nine rules for common-sense Wi-Fi.

1. Set your ultimate goals high for both your APs and all your devices: 802.11n, 5GHz, 40MHz bandwidth, four MIMO streams, WPA2-PSK (AES) on channel 36, 40, 44, 48, 149, 153, 157, 161, or 165. This will maximize your security stance, offer the highest maximum throughput, and set you up to encounter the least interference from other devices.

2. Keep your shopping list short and always check the documentation before you purchase. Many APs that support 802.11n won't support four MIMO streams. Others will support 802.11n, but only at 2.4GHz. The same goes for Wi-Fi devices. I once purchased an 802.11n camera and was eager to connect it to my 802.11n 5GHz network, but I couldn't because the camera was 2.4GHz only. This information was buried in the documentation, which I hadn't bothered to read in detail before tearing into the product.

3. Keep your passwords long. The longer your password, the longer it will take an attacker to crack it in a brute-force attack.

4. Keep your APs high. The higher your APs are physically, the further the signal they generate will travel.

5. Go downlevel only if you have to and only as far as you have to. You have a great 802.11n 5GHz network and everything is working fine—but then a new gadget that you need to get working only supports 802.11g at 2.4GHz, and your AP only works at 2.4GHz or 5GHz. You know you have to drop to 2.4GHz, but you should also consider setting your AP to block access to 802.11b devices because you won't be using them.

> The longer your password is, the longer it will take an attacker to crack it in a brute-force attack.

6. Scan your environment with a Wi-Fi scanner to see what other networks in your vicinity are using. If all the networks around you are on channels 36, 40, 149, and 161, you know exactly which channels not to use for your own network. Commercial and free software, such as inSSIDer for Windows and iStumbler for Mac OS X, is available.

7. Consider skipping SSID hiding. A common suggestion is to set your network name (SSID) to be hidden, so that a potential attacker can't see it. This also then requires that anyone who wants to connect to the network will need to know both the password and the exact SSID. Although it's true that attackers won't be able to see the name of your network, they will be able to see that a network is there—and a sophisticated attacker will be able to determine the SSID anyway.

8. Consider using MAC filtering. If you have a small number of Wi-Fi clients and don't typically add and remove devices, consider setting up a MAC filter list on your AP(s). Although this approach requires you to obtain the MAC address from each device and manually enter it in your AP's management software, it adds one more layer of complexity that an attacker has to go through before being able to connect to your WLAN because he must then spoof a valid MAC address. However, consider the added management overhead before you do this, especially if your WLAN contains a large number of changing devices.

9. Always think before connecting to a WLAN that's not your own. When you connect to a WLAN at a coffee shop, hotel, or a friend's house, always take a few seconds to think about what you intend to do on that network and balance that against the security in place. Remember that WEP encryption is basically no encryption, and much of what we do on the Internet is over unencrypted HTTP. However, if you only need to connect to a WEP-secured WLAN to go online with your 2048-bit encrypted VPN, you might feel perfectly comfortable doing so because the payload you will be passing wirelessly has a good level of encryption.

As always, none of this is a substitute for keeping your systems up-to-date and installing suitable anti-malware software and hardware or software firewalls.

Put Your New Knowledge to Use

Now that we've discussed the wireless landscape of today and gone over some basic rules for a high-performing and secure WLAN, take some time to see what you can do to get your own WLANs and APs up to the best level possible. Your iPads will thank you for the easy online access.

InstantDoc ID 140898



Michael Dragone (articles@mikerochip.com) is a contributing editor for *Windows IT Pro* and a senior network engineer. He holds MCDST, MCSE: Messaging, MCTS, and MCITP credentials and remembers when *Windows IT Pro* was called *Windows NT Magazine*.

Windows IT Pro Congratulates **Altova**

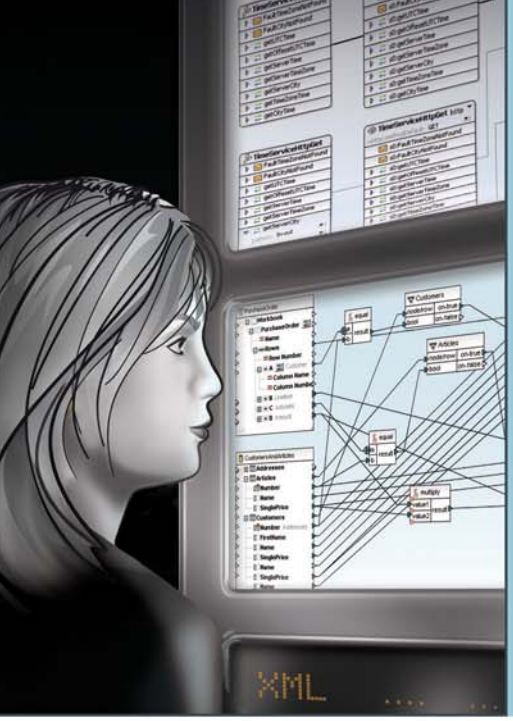
Windows IT Pro
Editors' Best Awards



Company: **Altova**
Category: **Interoperability**
Product: **Altova MapForce**
Award: **Editors' Best Gold**

ALTOVA®

Learn more about Altova here: www.altova.com • 978.816.1600



Connect legacy technologies affordably with the complete set of data integration tools from Altova®

ALTOVA® missionkit®

Experience how the Altova MissionKit®, the integrated suite of XML, data mapping, and database tools, can help you leverage existing technology and business software investments while integrating modern technologies – without breaking your budget.

NEW in Version 2012:

- Streaming reading/writing of files for large-scale ETL applications
- New data processing functions
- JDBC drivers (in addition to ADO and ODBC)
- New native Java APIs

The Altova MissionKit includes multiple intelligent tools for data integration:

MapForce® – Graphical data mapping, transformation, & conversion tool

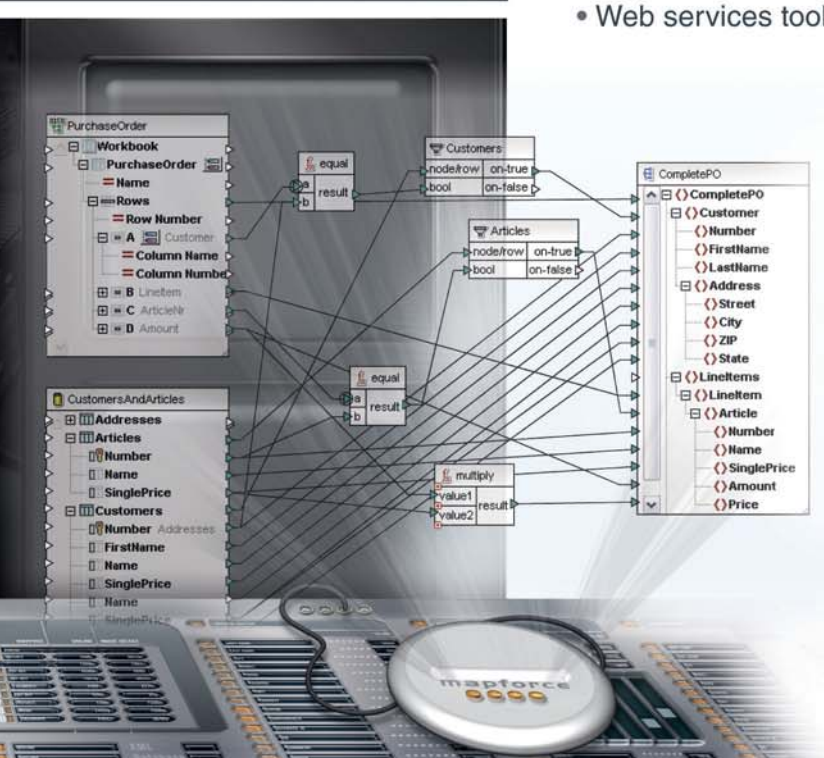
- Drag-and-drop data conversion with instant transformation & code gen
- Support for mapping XML, DBs, EDI, Excel®, XBRL, flat files & Web services

XMLSpy® – XML editor and Web services tool

- XML editor with strong database integration
- Web services tool, JSON <> XML converter

DatabaseSpy® – multi-database query, design & comparison tool

- Support for all major relational databases and translation between DB types
- SQL editor, graphical database design & content editor



Download a 30 day free trial!

Try before you buy with a free, fully functional trial from **www.altova.com**

Scan to learn more about data integration with the MissionKit.

FEATURE

Unleash the Power of Windows Phone



Free apps provide significant improvements to Windows Phone OSs

by Damir Dizdarevic

Ever since Windows Phone 7 was released, the number of available applications has been a serious concern. In addition to having some obvious functionality shortcomings in its initial release, first-generation Windows Phone 7 had very inferior application support compared with its main competitors, Google's Android and Apple's iOS. The number of applications on the Windows Phone Marketplace still doesn't match those available from the competition; however, you can now find some very good software for use with Windows Phone. In addition, Microsoft has released the first major upgrade for Windows Phone 7: Windows Phone 7.5 (formerly code-named Mango), which, according to Microsoft, provides more than 500 new or improved functionalities. According to the early feedback from end users, the new Windows Phone OS was worth the wait.

Previous Windows Phone 7 updates didn't bode well for a seamless and efficient upgrade path in the new release. Upgrade timing was very inconsistent for pre-Mango updates, which caused inconsistent customer experiences worldwide. Although some customers were able to install the NoDo and post-NoDo updates in March 2011, others had to wait until July or August. Feedback on the NoDo update process was quite negative.

But Microsoft seems to have learned its lesson. According to Windows Phone 7.5 deployment results in mid-October, things went much better—with the exception of Samsung Omnia 7 devices, which still can't use Windows Phone 7.5, and some limited issues with LG devices. Also, carriers seemed to be much better prepared this time. Most carriers started deploying Windows Phone 7.5 at the same time and didn't cause undue delays.

It's also good to see that even though Windows Phone 7 upgrades didn't go smoothly, developers didn't sit around idly, waiting for Windows Phone 7.5. The Windows Phone Marketplace now has more than 20,000 applications for Windows Phone 7, some of which significantly enhance the user experience.

Sync This, Sync That

Although Microsoft has never admitted to not including them, many of Windows Mobile 6.5's advanced features are missing from Windows Phone 7 (especially the release to manufacturing—RTM—version). For some of these mysteriously absent features, such as a unified Inbox or conversation view, the Windows Phone 7.5 upgrade provides a solution—but some of them can be compensated for with other applications. In addition, some features, such as support for digitally signed and encrypted messages, are still a no-go for Windows Phone 7, even with the latest upgrade to Windows Phone 7.5.

Personally, I very much miss the ability to sync all data from Microsoft Exchange Server, desktops, and online storage services. I'm an intensive Exchange tasks user, but Windows Phone 7 RTM doesn't support synchronization of tasks and notes from Exchange Server. In Windows Phone 7.5,

synchronization of tasks is enabled and integrated with the calendar. If you don't like the approach of integrating tasks with the calendar, you can find a few applications on the Windows Phone Marketplace that can provide this functionality. No free applications are available, but most apps provide you with a trial, so you can test Exchange connectivity and synchronization of tasks. Some applications have connectivity issues with various Exchange Server versions.

Based on user comments and my personal experience, APPA Mundi Tasks (www.appamundi.com/products/tasks) does a very good job. It lets you not only sync tasks from Exchange but also create new tasks and edit existing tasks on Windows Phone 7 devices, with various options. In addition, this app has its own live tile that can show the number of uncompleted tasks, which Windows Phone 7.5's synchronization of tasks doesn't offer. APPA Mundi Tasks has already had several upgrades, so most of the bugs are now fixed. You can get a 7-day trial, which is plenty of time to decide whether or not you like it. The full price is also quite reasonable, at $3.99.

Unfortunately, there's still no good application for syncing notes from Exchange Server. Although Windows Phone 7.5 does provide Out Of Office message management as a new advanced messaging feature, it still doesn't sync notes.

Syncing Microsoft OneNote notes stored on Windows Live SkyDrive with built-in OneNote mobile is possible. However, synchronization capabilities vary depending on which version of Windows Phone you're using. If you're still not using Windows Phone 7.5, synchronization is possible only in one direction—from device to server, by default. This means that you must create a note on your mobile device, then sync that note to your SkyDrive storage. However, OneNote mobile can't "see" notes that are already synced to your SkyDrive storage by using the OneNote 2010 desktop application. If you're using Windows Phone 7.5, you'll be able to see, edit, and sync all OneNote Notebooks that are located on SkyDrive. However, even though the OneNote application on Windows Phone 7.5 is enhanced, it still doesn't look as good as on iPhone (which uses the official Microsoft OneNote app).

If you aren't dedicated to Microsoft's OneNote solution, you can also try Evernote. An excellent free Windows Phone 7 client for Evernote is available (www.evernote.com/about/download/windowsphone.php). It fully uses a Metro-style interface to sync notes between all platforms where Evernote is installed. On Windows Phone 7, Evernote lets you insert pictures in your notes and connect your GPS location with a note. If you need notes on a mobile device, you should definitely try this app.

When it comes to cloud-based storage, Windows Phone 7.5 provides full SkyDrive support from the Microsoft Office hub—but if you want some other web-based storage on your Windows Phone device, the only alternative is Dropbox (www.dropbox.com). The application Simple Dropbox Viewer does a pretty good job of accessing content from your Dropbox account, and it's completely free. Unfortunately, you can't use this app to send anything from your phone to Dropbox storage.

If you can buy applications from the Windows Phone Marketplace, you should consider Neologics' BoxFiles for Dropbox (www.dropbox.com/apps/6665/boxfiles-for-dropbox), which provides some additional functionality for a very reasonable price. This app lets you manage files already on your Dropbox account, create new folders, and upload pictures (which is currently the only file format supported for upload). You can download a free trial for testing, or you can buy the full application for only $1.29. So far, this app has excellent ratings on the Windows Phone Marketplace. It's available as a trial, and you can even use it without a time limit with somewhat reduced functionality. In a new version, this app also provides access to SkyDrive, so you can have a single point of management for multiple storage solutions.

If you're using Google Docs, the Windows Phone Marketplace offers a pretty good client for free. This application is called GDocs and is available at wp7.apphab.com/?s=GDocs. A big limitation of this application is that it only lets you view existing files.

Another application that supports syncing is Password Manager, by Davide di Bernardo (wp7.apphab.com/password-manager-by-davide-di-bernardo). This free application lets you securely store your passwords (for various services) on a Windows Phone 7 device; it also lets you store a backup encrypted password database on your SkyDrive account.

A similar solution that supports multiple platforms is also available. The 1Password application (agilebits.com/products/1Password) can work across several desktop and mobile platforms.

Going Social

One of the great things about Windows Phone is its integration with social networks. In addition to merging contacts from various services into one contact list, Windows Phone 7.5 also integrates with Facebook, Twitter, and LinkedIn by default. I think this is the best natively implemented integration that you can find in a device. (You can also install the official Windows Phone Facebook application for some additional functionality, although the Facebook app still looks and works better on Google's Android and Apple's iOS.)

Windows Phone 7.5 also provides Windows Live Messenger integration inside the Messaging hub, which also gives you the ability to chat over Facebook. If you don't like this approach of integrating text messages with Live Messenger and Facebook chat, you can try the free *Messenger by Miyowa* application (www.miyowa.com/Messenger-by-Miyowa.html). This application works very well, especially after being updated.

Those who want a separate Facebook chat app will find the Facebook Instant Messenger (Fim) application (www.mosko.mobi) useful, although it can't integrate with the real Facebook application or with Windows Phone 7's People tile. If you like geo-tagging and using Foursquare, there's a free application called 4th & Mayor (www.4thandmayor.com/index.html). Interestingly, this app is far more popular on Windows Phone 7 than the official Foursquare application. It also provides much more functionality. For sharing pictures, Yahoo's official Flickr client is free and available from the Windows Phone Marketplace.

There's an official Twitter application for Windows Phone 7 that does a pretty good job, although the Windows Phone Marketplace offers several other Twitter clients. For example, Rowi [lite]

(windowsphone.com/en-US/apps/5da58f1f-562e-e011-854c-00237de2db9e) is a free and highly rated Twitter client. Windows Phone 7.5 does provide full Twitter integration, but some people still like to use their favorite application.

LinkedIn users can also find clients for Windows Phone 7 devices. Starznet's Link Me In (www.starznet.co.uk/wp/linkmein.aspx) isn't as good as Android's or iOS's LinkedIn client, but it's free and can be used for basic functionality. An official LinkedIn application is still missing, but because Windows Phone 7.5 has native LinkedIn support, I wonder if we will see one at all.

In addition to applications that support specific social networking services, you can also find several applications for accessing specific forums, websites, and so on. For example, XDA Developers (www.xda-developers.com), which is a popular portal for smartphone users, has its own application for forum access. If you're using WordPress for blogging, I have some good news for you—the Windows Phone Marketplace offers a free WordPress client for Windows Phone 7.

Multimedia Support

The Zune client that's implemented in Windows Phone 7 is good. But if you want additional functionality, such as Smart DJ support, additional tools are also available.

Windows Phone 7 has a built-in YouTube "application"—but it actually just provides a link to the web-based YouTube Mobile application. Until Microsoft enhances this feature, you can use the free LazyTube (www.lazywormapps.com) app. This full-featured YouTube client has a good interface and performance. A paid version of the app can provide HQ playback, but the free client is more than enough. A disadvantage is that you can't make LazyTube your default YouTube client—if you click a YouTube link, it opens in the default Windows Phone 7 app. As an alternative, you should consider SuperTube (wp7.apphab.com/supertube-by-fast-code). In addition to playing YouTube videos in standard and high definition, this application also lets you download videos from YouTube, as well as continue broken downloads.

If you like radio, you should definitely check out TuneIn Radio (wp7.apphab.com/tunein-radio-by-radiotime). This Internet-based radio service client provides several thousand radio stations worldwide. It's also free and very easy to use and navigate.

Shazam, which is a popular app on other platforms, is also available for Windows Phone 7 (www.shazam.com/music/web/wp7.html). The basic version is free; Shazam Encore provides some additional features and unlimited tagging. In Windows Phone 7.5, you can also use Bing search for similar functionality as with Shazam.

Books and e-Zines

Although long-term reading on a mobile device might not be very pleasant, some people consume a lot of content from their phones—especially if they have screens like that of T-Mobile's HTC HD7 or HTC Titan. Windows Phone 7 provides good application support for these resources. Adobe Reader was one of the first applications available on the Windows Phone Marketplace; it lets you open PDF files with almost the same functionality as on other platforms. If you're into books, Amazon provides a free Kindle application for Windows Phone 7 devices. There's also a good Wikipedia app.

For those who love movies, search the Windows Phone Marketplace for the IMDB application. This free app makes great use of the Metro interface concept. Movie fans will have a lot of fun with the app.

If, like me, you frequently visit portals for technology freaks, you'll have plenty of choices on Windows Phone 7. Many popular portals such as AOL's Engadget and Gawker Media's Gizmodo have applications on the Windows Phone Marketplace. There are also several applications that concentrate information from various news sources. One of the best ones is TechRack; it covers a lot of news sources and has a good interface. Weave is also worth considering. (Both TechRack and Weave are free.) Paul Thurrott and his Supersite for Windows also have a Windows Phone 7 application (www.windowsitpro.com/mobile-apps).

If you're a frequent visitor of Microsoft events or websites, the Windows Phone Marketplace has a lot to offer you—and most of it for free. You can find a Windows Phone 7 application for almost every important Microsoft event (e.g., TechEd, TechDays). In addition, there are applications for the Exchange Team Blog, Born to Learn (part of the Microsoft Learning Community and Evangelism Team), and several others.

Navigation

At present, there isn't much to say about Windows Phone's navigation capabilities. A built-in Maps application can provide basic navigation functionalities, but with limited coverage. This app relies on Bing Maps and requires an Internet connection during use. It doesn't provide voice navigation.

In mid-October, Navigon released the first real GPS application for Windows Phone 7. It currently provides offline maps for the United States and a good part of Europe and is available for the very reasonable price of $29.99 (USD, for US maps). However, because the Windows Phone Marketplace still isn't available in many countries worldwide, many users will still be without a real GPS application. A limited version of Navigon's software is available to German T-Mobile users who purchase Windows Phone 7 devices.

As an alternative, you can also try Mobile GMaps. This free application uses Google Maps and does a pretty good job—although it's still in the testing phase.

Free Enhancements

Application support for Windows Phone has been significantly improved in the past year. Except for navigation, an average user can find all the necessary apps on the Windows Phone Marketplace—and most of them are free. Several good paid applications are also available, although availability depends on the region where you reside, which can be a problem. But even using only free applications, you can greatly enhance the capabilities of Windows Phone.

InstantDoc ID 140130



Damir Dizdarevic
(ddamir@logosoft.ba), manager of the Learning Center at Logosoft in Sarajevo, Bosnia, has published more than 380 articles in various IT magazines. He's an MVP for Windows Server Infrastructure Management, and an MCSE, MCTS, MCITP, and MCT. He's also an author of several Microsoft Official Courses and a frequent speaker at Microsoft conferences in Europe.

SharePoint 2010 Goes Social, Part 3

Building on the user profile

by Kevin Laahs

This is the last article in a three-part series that discusses social networking with SharePoint Server 2010. In "SharePoint 2010 Goes Social, Part 1" (www.windowsitpro.com, InstantDoc ID 129949) and "SharePoint 2010 Goes Social, Part 2" (www.windowsitpro.com, InstantDoc ID 136368), I described the importance of the user profile and how to synchronize it with Active Directory (AD). In this article, I describe the major features that build on the user profile to leverage an often forgotten information source—its people. Note that the social networking features described in this series are available only with a SharePoint Server 2010 installation. They aren't available in a SharePoint Foundation 2010–only deployment.

As mentioned in the previous articles, it's crucial to have a rich user profile, which means that everyone needs to be willing to enter details about themselves and the projects they're working on so that other people can discover this information and build linkages out of it. Some of this information can be imported from other information sources (such as synchronizing the user profile with AD), but generally it's the users themselves who know what skills they have and what they're working on.

The SharePoint designers know that most people generally won't go out of their way to provide such information. And if they do provide it, they tend to be fairly lethargic in keeping the information up-to-date. This is why SharePoint provides tools that are geared toward automatically keeping certain information up-to-date and presenting the user with opportunities to update other pertinent information in a seamless and simple fashion. I'll now describe the major tools that can help people discover "who knows who," "who knows what," and "who is doing what," which results in a vibrant and therefore worthwhile social network.

My Site at the Center

Assuming your organization wants to fully leverage SharePoint's social networking features, every user will have what is known as a *My Site*. There are three feature areas that are delivered through My Site, and there are permissions that control the availability of these features. By default, these permissions are enabled for all authenticated users. You can customize these permissions by using the Manage User Permissions option in the User Profile Service application, which you can access through the SharePoint Central Administration site. The permissions are as follows:

- Use Personal Features. This permission lets users advertise details about themselves to others through their public profile pages. Users can also maintain some of the displayed details (e.g., About Me information) and control certain aspects of the details (e.g., who is allowed to view them). Users can access this feature set from the My Profile tab in their personal home pages.
- Create Personal Site. This permission lets users create a standard team site for their own use. In this site, users can store personal documents and documents that they want to share with others. Users

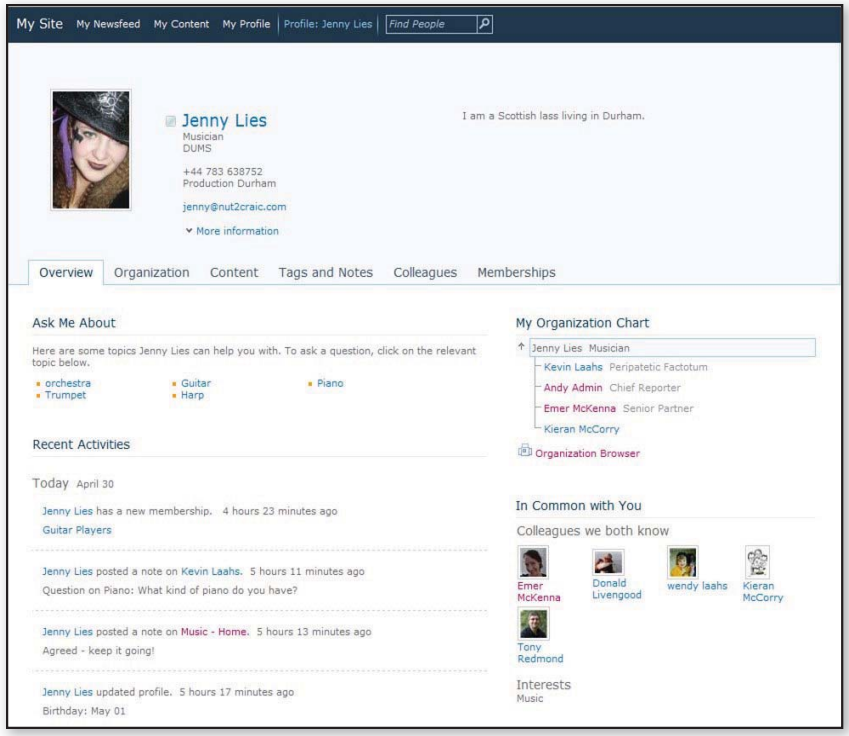


Figure 1: Viewing another person's profile page

can access this feature set from the My Content tab in their personal home pages.

- Use Social Features. This permission lets users use social features (e.g., social tagging, colleagues) and have an activity feed that shows their colleagues' recent activities. Users can access these features from many places, including the My Newsfeed tab in their personal home pages.

Users can quickly access their personal home pages on My Site by clicking their names in the top right corner of most SharePoint pages. This reveals a drop-down list that includes links to their personal home page and public profile. As users navigate in particular areas of SharePoint, many of the links that they'll encounter will take them to the public profile of other users. For example, if a search result relates to a person, the search results will link to that person's profile page.

My Profile Page

The page that renders the profile page is named person.aspx, and it resides in a site collection known as the My Site Host. Each User Profile Service application is associated with one My Site Host. You can control the My Site Host with the Setup My Sites option in the Settings page of the User Profile Service application. If you want to change the default location for the My Site Host, you need to use the My Site Host site template or a blank template to create the site collection where the My Site Host will reside. You also need to make sure that the site actually exists at the top level of the Web Application that's used for the My Site Host. Otherwise, people won't be indexed by the search engine.

Person.aspx is a multi-tabbed page. The details it displays depends on who the requesting user is and the query strings passed to the page. If person.aspx is called with no query strings, the profile of the current user is displayed. However, the page is also used to show the public profile of users to other users. In this case, the details that are displayed depend on the relationship that exists between the two users. For example, Figure 1 shows the result of the user named Kevin Laahs viewing the profile of the user named Jenny Lies. In this case, the person.aspx page was called as follows:

```
http://<My Site Host>/person
   .aspx?AccountName=laahs\jenny
```

The profile's Overview tab displays things that the two users have in common, such as the colleagues they both know and interests they both enjoy, in the "In Common With You" section.

Each user can control what information other people can see. For this to work, the relationship between the calling user and target user is determined; that determination places the calling user into one of the following groups:

- My Manager. The calling user is listed as the manager in the target user's profile.
- My Team. The calling user is listed in the target user's colleague list, and the My Team column is set to Yes.
- My Colleague. The calling user is listed in the target user's colleague list, and the My Team column is set to No.
- Everyone. None of the conditions are true.

In the user profile, each property has a default value and a privacy setting that defines the group that's allowed to see it. If users are allowed to change the property's privacy setting, they can do so by editing their profile and changing the group that's allowed to view the property. In addition, users can toggle the view of their own profile to see what it will look like from the perspective of someone else. This is done using the *View my profile as seen by* option at the top of the profile page.

This privacy feature extends to more than just user profile properties. Users can also control who can see their site and group memberships and who can see their colleagues. Policies are used to control the objects subject to privacy settings and whether default settings can be overridden by users. Administrators can manage these policies using the Manage Policies option in the Settings page of the User Profile Service application.

By maintaining their profiles and keeping properties such as Interests and Skills up-to-date, users make a crucial contribution to the organization's intellectual wealth. These properties let users find expertise quickly and build the linkages that make up the social network within an organization.

Six Tabs Over My Site

As you can see in Figure 1, there are six tabs on the profile page. Some of the highlights of these tabs are as follows.

Overview tab. In addition to the "In Common With You" section I mentioned

previously, the Overview tab shows the user's position in the organizational hierarchy, recent activities, skills, and interests. The latter gives visiting users the ability to quickly ask the user about such interests. This action writes a note on the user's note board, which subsequently finds its way into the user's newsfeed. Every user has a note board that functions in much the same way as a Facebook wall.

Organization tab. On this tab, visiting users can explore in more detail the user's position in the organizational hierarchy. If the browser has Microsoft Silverlight support enabled, visiting users can take advantage of the visual interface shown in Figure 2 to hone in on individuals to see the organizational hierarchy from their perspective.

Content tab. This tab shows recent content that was authored by the user. The content includes blog entries and documents the user authored across the SharePoint farm. The Content tab also lets visiting users quickly hone in on collateral from a specific SharePoint site because it lists each site that contains content authored by the user.

Tags and Notes tab. SharePoint lets users tag web pages with keywords and add notes and ratings. This tab shows the user's tag clouds and recent notes and activities. Clicking a tag term displays the note and activities with which that tag was associated. This facilitates the "wisdom of the crowd" because popular items rise to the surface.

Colleagues tab. In this tab, users can manage their colleagues list.

Memberships tab. This tab shows details of the groups the user is a member of. For example, it shows the SharePoint sites and AD Distribution Groups (DGs) the user is a member of. Note that this only shows SharePoint sites where the user is explicitly added to the SharePoint group that represents the site members. This is an important point because a user can be a member of a SharePoint site through many other routes, such as being an Owner or being a member of an AD Security Group that has been added to the Members group of a site. The sites that a user is a member of are updated by a background job called *User Profile Service Application - User Profile to SharePoint Full Synchronization,* which runs hourly by default. You can force this job to run as needed in Central Administration.

Colleagues Are Important

Many of SharePoint's social features rely heavily on knowing who a user considers a colleague. Armed with this knowledge, SharePoint can establish relationships between people, such as the social distance between them. This can help build stronger social networks. For example, you might not know a particular person but you can be informed if one of your colleagues (or one of your colleagues' colleagues) knows that person. This would allow you to ask your colleague for an introduction to the person.

Each user has a list of colleagues that's maintained automatically and manually. By default, users who have the same manager listed in their user profiles are automatically added as colleagues and marked as being a member of "My Team." This is one example of how the colleague list is automatically maintained.

Suggested colleagues are also automatically generated if you install the Microsoft SharePoint Server Colleague Import Add-In for Outlook 2010. Suggested colleagues are derived from users' messaging habits in terms of who they have been sending email to and receiving email from. The add-in scans each user's Sent Items folder to look for names (colleagues) and keywords (expertise) along with the frequency of those names and keywords.

The results of these scans are used to update a file named spscoll.dat in each user's Windows profile. This file contains a list of email addresses and a ranking to determine how much the user has been communicating with other people. This list of suggested colleagues is imported to SharePoint, where it will be displayed the next time users visit the Colleagues tab on their personal home pages.

Although the suggestions are imported, users have to decide which colleagues they want to add to their colleagues list and which keywords they want to add to their list of expertise areas. Therefore, this is an opt-in feature, which is sensible from a security and privacy perspective. Note that the email addresses contained in the suggested colleagues list must also already exist in the SharePoint user profile for users to be able to add them as colleagues. Microsoft Office Communicator also contributes to the suggested colleagues list by analyzing IM practices.

SharePoint makes it easy for users to manually add colleagues by providing one-click links in appropriate places, such as search results that contain people. Another place is through the Outlook Social Connector. This Outlook 2010 feature lets users hook up to external social networks (e.g., Facebook, LinkedIn) and display

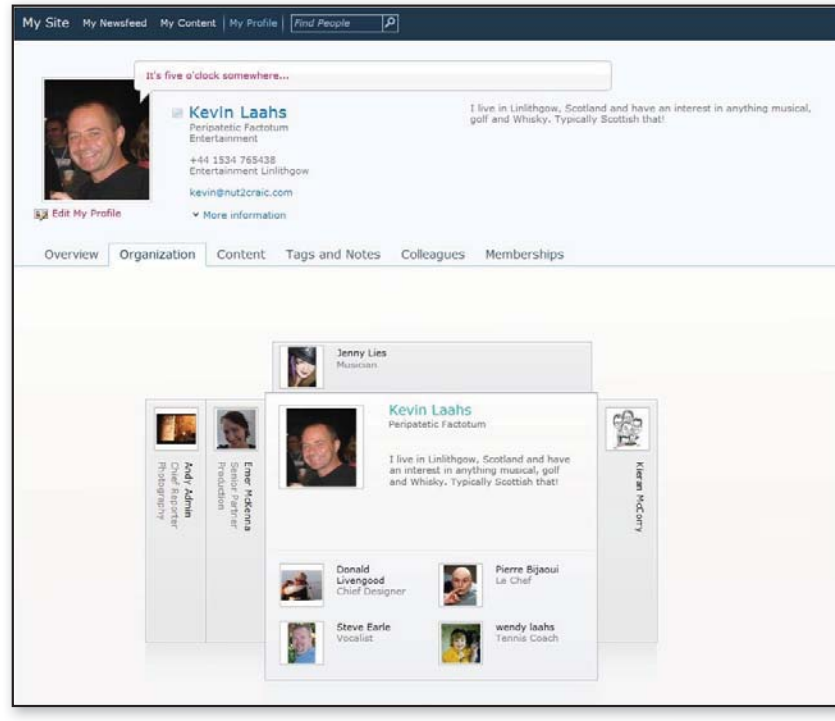


Figure 2: Exploring a user's position in the organizational hierarchy

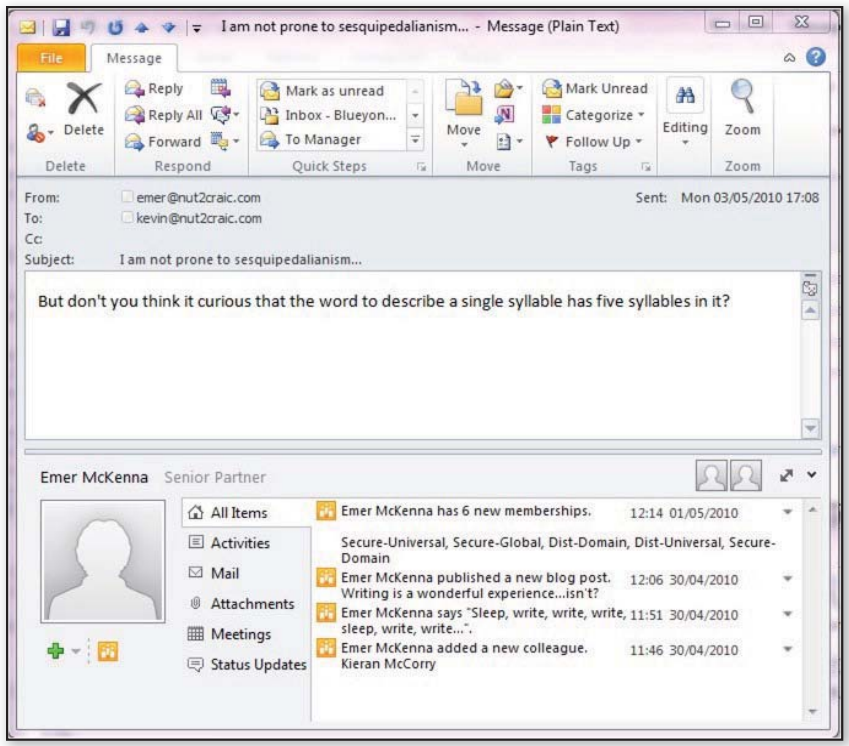


Figure 3: Using the Outlook Social Connector to display information from social networks

information from those social networks directly in Outlook. My Site is the only out-of-the-box connector. After it's configured, users can simply add colleagues from the social connector pane at the bottom of each Outlook message window. This pane also shows information from the social network, as Figure 3 shows. In this case, the sender's activity is displayed.

What Are People Up To?

The My Newsfeed page (which is accessed from the horizontal menu at the top of the profile page) is where users can keep up with what others have been doing, as Figure 4 shows. The idea here is that if your colleagues are showing interest in something, there's a high likelihood that you'll benefit from knowing this. For example, if a colleague tags some content with a tag that relates to your interests, you'll want to investigate that content. You are, therefore, leveraging the activities of your colleagues to keep yourself informed of important information. This is clearly leveraging the community, which is a core tenet of social networking.

Implicit and explicit activities relating to your colleagues are listed in the My Newsfeed page. Implicit activities are actions that users didn't perform themselves but that affected them. For example, a user might have been added as a member to a new SharePoint site or a user's reporting relationship might have changed, resulting in new peers being created. Explicit activities are actions that users performed directly, such as commenting on someone's note board or updating their interests and expertise areas.

Users control what activities they want displayed in their My Newsfeed page by editing their own profile and selecting the activities to monitor. There are sixteen activities that users can choose to monitor, including tagging of content by a colleague, one of their interests being used as a tag, colleagues authoring new blog content, new colleagues, manager changes, and upcoming birthdays.

Each user's newsfeed is updated by a background job called *User Profile Service Application - Activity Feed Job,* which runs daily by default. You might want to increase the frequency of this job if you want to capture activities in a timelier fashion. This can be done using the *Check job status* option in Central Administration.

Newsfeeds add value only if everyone participates in keeping their profile information up-to-date. Otherwise, newsfeeds become stale and add no value to the overall intellectual wealth of the organization. Every month, SharePoint sends emails to users, reminding them to keep their profile vibrant and up-to-date. (This is a scheduled job that you can disable in Central Administration if you don't want to send out these emails.) There are seldom good technical solutions to increase participation, so it's in your best interest to lead by example and constantly encourage people to keep their profiles up-to-date.

Searching for People

Out of the box, SharePoint 2010 provides a search landing page that's tailored to show

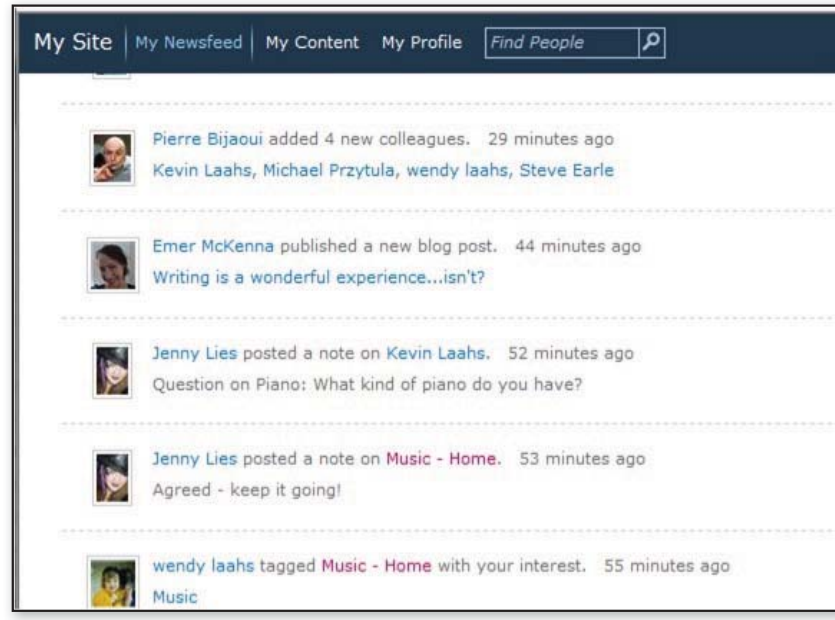


Figure 4: Using the My Newsfeed page to keep up with what others have been doing

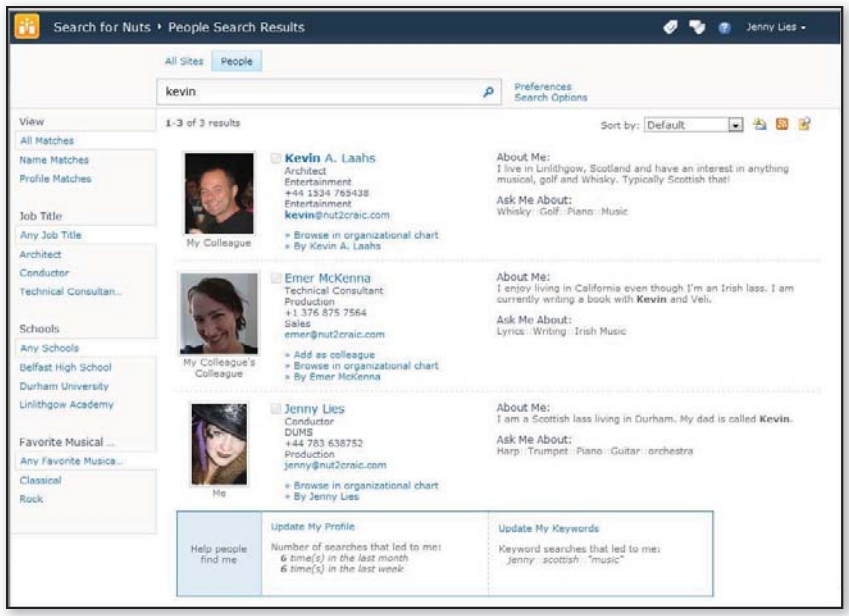


Figure 5: Using the People Search Results page to see pertinent information about people

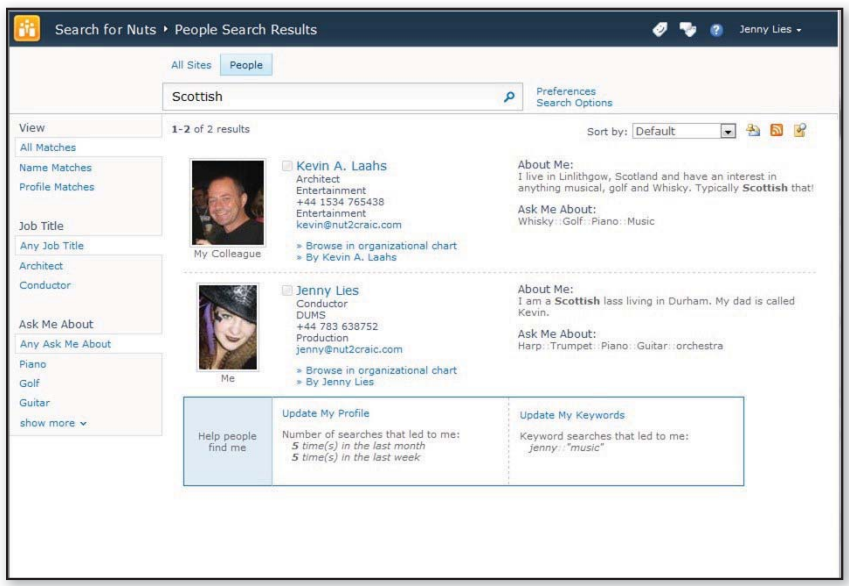


Figure 6: Discovering mutual interests in the People Search Results page

pertinent information about people. For example, it might display the interests that are most common among the people displayed in a search's results. This page's filename is peopleresults.aspx and it's the landing page associated with the People tab on the default search results page, as Figure 5 shows.

Two interesting Web Parts in people results.aspx are the People Search Core Results Web Part and People Refinement Panel Web Part. The People Search Core Results Web Part uses the Local People Search Results search location. You can modify the Web Part to override the default properties that are returned for this location or modify the Extensible Style Language (XSL) so that the results are displayed in a different way. This Web Part supports the following interesting features:

- Social distance. The results show the social distance between the user performing the search and the users returned in the result set by displaying the relationship underneath their pictures. For example, as Figure 5 shows, the relationship might be listed as "My Colleague" or "My Colleague's Colleague." The latter can help users get an introduction to someone through one of their colleagues.
- Vanity search. A vanity search is when the user performing the search shows up in the search results. This usually occurs when users deliberately search for themselves. Vanity search results show users how many times other people are clicking through to their names and what keywords are being used to find them. This information appears at the bottom of the search results, as Figure 5 shows. If users see that they're not being clicked much, it might encourage them to keep their profiles up-to-date and contribute more to the organization. In line with the design goal of making it easy for users to keep their information up-to-date, there's one-click access to take users to their profiles.

The People Refinement Panel Web Part displays suitable refiners based on the search results. Unlike the refinement Web Part for the normal search results page, you can't modify the refiners that are ultimately displayed in the people results page. However, SharePoint does a pretty good job of showing you the most relevant refiners based on the result set, as you can see in the left navigation pane in Figure 5 and Figure 6.

Figure 5 returned more users that had less in common with each other than Figure 6, so the refiners were Job Title, Schools, and Favorite Musical Instruments. In Figure 6, the two users returned had some mutual interests, so these were displayed as refiners. Clicking one of the interests would then find all the people in the organization who shared that interest. This key feature lets users find expertise quickly and, as I mentioned previously, works only if people keep their profiles up-to-date.

Being Social

SharePoint does do social. However, if you want to do it well, you must embrace and promote a culture where people willingly and regularly update their user profiles with rich and relevant information.

InstantDoc ID 139482



Kevin Laahs
(kevin.laahs@hp.com) is a technology strategist with HP Enterprise Services. He's coauthor of four books on SharePoint; the latest is *Microsoft SharePoint 2010 All-in-One For Dummies* (Wiley).

Windows IT Pro Congratulates **TrainSignal**

TRAINSIGNAL

THE GLOBAL LEADER IN PROFESSIONAL COMPUTER TRAINING™



Community Choice Gold

Category: **Training/Certification**

Product: **TrainSignal**
Computer Training

Learn more about TrainSignal here: www.TrainSignal.com/ITPro • 888.520.1812

TRAINSIGNAL

THE GLOBAL LEADER IN PROFESSIONAL COMPUTER TRAINING™

Put Our Award-Winning Training to Work for Your Entire IT Department



Online Learning Portal

All the Courses You Need in One On-Demand Package

$4,995

for 5 users

Learn More At

TrainSignal.com/ITPro

Get over 40 IT Certifications

Superior Training

Web-Based Access:
No Software, No Hardware, No Headaches

Available 24x7 Anywhere, On Any Device

Monitor Usage and Results

Accessible on **iOS** & **Android** Devices

Track Users With Reports On **Your Custom URL Portal!**
companyname.mytrainsignal.com

INCLUDED Training Topics

Microsoft · Cisco · CompTIA · VMware · Citrix · Microsoft Office

Industry Leaders trust us:

Cisco · ADP · DELL · IBM

Contact us:
1.888.229.5055
Worldwide: **1.847.776.8800**
zach@trainsignal.com
www.trainsignal.com

Copyright © 2002-2011 TrainSignal, Inc. All Rights Reserved. All logos and trademarks are property of their respective owners.

- up.time software
- Network Instruments
- GFI Software
- ARCHOS

Visage Adds Daily Insight to the MobilityCentral Enterprise Mobility Management Suite

Visage Mobile introduced a new component, called Daily Insight, to its cloud-based MobilityCentral Enterprise Mobility Management Suite. Daily Insight gives enterprise mobility managers the opportunity to stop cost overruns or device misuses before they get out of control. Working in concert with the range of features already available in MobilityCentral, Daily Insight offers faster access to a broader scope of data, daily updates by device and device attributes, daily insights into data usage as measured against monthly billing cycle plans, and daily visibility into roaming, application downloads, and application deletions down to the employee level. Current MobilityCentral subscribers can immediately upgrade their subscriptions to include Daily Insight, while new customers can now subscribe to the entire, broader suite. For more information about MobilityCentral Daily Insight, visit www.visagemobile.com/dailyinsight.



ARCHOS G9 Tablets Launch with Android Honeycomb 3.2

ARCHOS announced the availability of its new G9 Android tablets. The 8" ARCHOS G9 tablet is an Android Honeycomb 3.2 tablet featuring an OMAP 4 processor with an ARM Cortex dual-core A9 at 1GHz for $299. The ARCHOS G9 "Turbo" will use the OMAP 4 dual-core processor up to 1.5GHz. Android Honeycomb 3.2 is specially designed and optimized for tablets, giving a full web experience for on-the-go web browsing, communication, and applications. Adobe Flash 10.3 support brings the true web experience. ARCHOS G9 tablets will include access to Android Market, which has more than 250,000 applications available for download. ARCHOS G9 tablets also come with a suite of Google mobile applications, including Google Talk with video chat, Gmail, YouTube, Google Maps, and Google Calendar. ARCHOS G9 tablets are available with flash storage and 250GB hard drive storage capacities. For more information about the tablets, contact ARCHOS at www.archos.com.

PRODUCT SPOTLIGHT

"Set it and Forget it" Real-Time VMware Monitoring with up.time 6

uptime software announced version 6 of its award-winning up.time software platform, delivering automated, real-time monitoring of VMware, and providing virtual server and application capacity-management capabilities from a single integrated dashboard. In addition to new VMware monitoring and reporting capabilities, up.time 6 continues to deeply monitor across all data-center infrastructures and applications, delivering a complete set of performance, availability, and capacity metrics. A key differentiator of up.time 6 is its per-physical-server licensing. This model allows customers to use as many instances as they want on licensed servers at no additional cost. Additionally, up.time 6 offers full control and deep monitoring over servers and applications across Windows, UNIX (IBM AIX, Sun Solaris, HP), Linux, VMware, Novell, and more—from a single dashboard.

With up.time 6, uptime software also introduces "Set it and Forget it" scalable VMware monitoring; Real-Time vSync (VMware Sync) for auto-discovering thousands of virtual machines (VMs) in seconds, offering full dashboard visibility into a VMware environment; Sprawl Control, which provides proactive and reactive sprawl-killing capabilities; Virtual Machine Power Awareness, smart monitoring that understands the power state changes in a Data Protection Manager (DPM) server and eliminates false alerts when dynamic systems are in maintenance; Deep VMware Capacity Metrics; Global VMware Capacity Reporting for comparing historical capacity trends across all VMware assets; and Virtual Capacity Forecasting of future capacity or storage so IT isn't blindsided by unexpected capacity needs. To learn more about uptime software, please visit www.uptimesoftware.com.

Quest OnDemand Migration for Email Moves Email to the Cloud

Quest Software now offers a solution that helps organizations migrate from on-premises Exchange Server or Google Gmail environments to the Microsoft Office 365 cloud email platform, enabling them to take advantage of the functionality and convenience presented by the cloud. Quest OnDemand Migration for Email moves users and data simply and securely, without requiring companies to install or maintain software for the move. The Quest OnDemand Migration for Email Administrator Edition provides multi-threaded migration to support multiple, simultaneous migrations; the flexibility to migrate email, calendars, and folders in a phased approach; data filtering to clean up

QUEST SOFTWARE®
Smart Systems Management

unwanted data and complete the migration faster by filtering email data and calendar events by age; and mailbox authentication by authorized administrators who can migrate user mailboxes without knowing or resetting user passwords. For more information, go to www.quest.com.

GFI VIPRE Antivirus Business 5.0 Simplifies Malware Defense

GFI Software launched GFI VIPRE Antivirus Business 5.0 and GFI VIPRE Business Premium 5.0, the latest evolutions of the company's flagship antivirus solutions. GFI has made several key enhancements to VIPRE Business, including incompatible software removal (enables admins to deploy VIPRE Business in an environment free of other antivirus agents), Windows Firewall auto-configuration (automatically configures and provisions Windows Firewall settings on all endpoints to ensure communication with all deployed VIPRE agents), integrated database (eliminates the need for any database configuration by admins), auditing and reporting (aids in policy enforcement, regulatory compliance, and e-discovery), remote management, and an enhanced management console. To learn more about VIPRE Antivirus Business or VIPRE Business Premium, visit www.gfi.com.

GFI

Network Instruments Launches Newly Architected Observer Platform

Network Instruments announced the latest version of its Observer performance-management platform, which significantly expands support for complex communications and multi-tiered application environments. Developed in response to customer demand, Observer 15 focuses on critical application challenges that IT teams face in validating video conferencing performance, gaining insight into the middleware layer of multi-tiered applications, and proactively tracking end-user experience without the burden of agents. The redesigned platform also addresses the primary challenges IT managers face in deploying performance management systems in the data center: network overhead and scalability limitations. Observer 15 includes comprehensive video-conference monitoring, Microsoft UC analysis, IBM WebSphere MQ analysis, new metrics and intelligence for measuring end-user experience, several high-speed capture and analysis innovations, and new probe-centric analysis, streamlined app management, and more. For more information, visit www.networkinstruments.com.

LogLogic Announces Free Windows Log Collector

LogLogic announced the next generation of the Lasso Enterprise Windows event collector. The new release, version 2.1, is available as a snap-in to the Microsoft Management Console (MMC). New enhancements include improvements to stability and performance, as well as a new download page. Lasso Enterprise is unique in that the solution can convert Windows events registered with the Windows Event Service to industry-standard syslog format, for distribution and forwarding to compliance, security event management, and IT operations solutions. This feature makes Lasso Enterprise an ideal solution for organizations that need to collect Windows events, yet do not want to be bound by proprietary solutions. Lasso Enterprise 2.1 is available now for free download at www.loglogic.com/lasso-enterprise. Find more product information at www.loglogic.com/lasso.

Lasso Enterprise

Paul's Picks

www.winsupersite.com



SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Windows Phone 7.5

PROS: Tons of new features; deep Facebook and Twitter integration; Local Scout

CONS: New phones using 7.5 features slow to roll out; some features available only on those non-existent new phones

RATING: ◆◆◆◆◇

RECOMMENDATION: For Windows Phone 7.5, Microsoft performed fit and finish updates and added major, useful features. Key among them is Local Scout, which finds the best restaurants, shopping, and other places of interest nearby. It also includes better Facebook integration, Twitter and LinkedIn integration, a new web browser, and better platform capabilities. Some new features, such as Internet sharing and visual voice mail, will only be available with new devices at first, and then only when supported by the wireless carrier. Still, it's the nearly perfect mobile OS, and far more innovative than Apple's and Google's offerings.

CONTACT: Microsoft • www.microsoft.com

DISCUSSION: "Windows Phone 7.5 Review," www.winsupersite.com/article/windows-phone-7/windows-phone-75-review-140726

Apple iPhone 4S

PROS: Typical Apple quality; appears to fix attenuation issues; high quality camera

CONS: Small screen; tired design; not much of an upgrade for iPhone 4 users

RATING: ◆◆◆◆◇

RECOMMENDATION: Apple's iPhone 4S looks like its predecessor, which is problematic for anyone looking to upgrade. But for iPhone 3GS users, the iPhone 4S is a no-brainer: Apple has apparently fixed the signal attenuation issues via software, and the 4S offers faster processing and graphics. Coupled with useful improvements such as iOS 5, a better camera, and the best-ever ecosystem of apps, content, and accessories, and you have the makings of a stealth hit. The Siri voice-control system is still in beta but boasts significant improvements over previous voice-control systems.

CONTACT: Apple • www.apple.com

DISCUSSION: "Apple iPhone 4S," www.winsupersite.com/article/iphone/apple-iphone-4s-140970

InstantDoc ID 140997

INSIGHTS FROM THE INDUSTRY

Top 10 Reasons SMBs Fail to Back Up Their Data

Loss of data ranks as a "worst nightmare" for businesses of any size, but for small-to-midsized businesses (SMBs), data loss can be especially catastrophic: The Federal Emergency Management Agency (FEMA) even estimates that 40 to 60 percent of SMBs never re-open after a data disaster. So, considering the threat of natural disasters, hardware and software failures, and worker recklessness leading to catastrophic data loss, why do some SMBs still fail to back up their data? Matthew Dornquast, CEO of Code 42 Software, shared this list of the top 10 reasons SMBs fail to back up their data, along with his response to each.

Excuse #1: It Costs Too Much

With a wide selection of options on the market, data backup has become increasingly affordable when it comes to protecting your company's files. More important, compared with the costs of data loss (expenses related to loss of productivity, decreased quality, disk recovery costs, lost intellectual property, and so on), backup solutions are one of the most cost-effective decisions you can make. With some backup solutions, customers can recover their yearly costs by restoring data from just one laptop.

Excuse #2: It Takes Too Much Time to Manage

There are backup solutions that run automatically and continuously without requiring any intervention from the user. SMBs can set up an account and then let it run in the background and forget about it.

Excuse #3: It Isn't Worth the Effort to Back Up

Even businesses with the most tangible of services have important information on their computers. While important documents and financial records might exist in other forms (emails or paper files, for example), tracking down your work can still take a lot of time. When deadlines loom, it might be time that you can't spare. Even if you find the lost files, they might not be the correct version, or they might be damaged by a virus or otherwise inaccessible.

Excuse #4: It Slows Down My Computers!

Most good high-performing backup software runs automatically and continuously without slowing you down, even on laptops. Technologies such as data deduplication and incremental backups reduce demand on CPU resources, network bandwidth, and storage costs.

Excuse #5: It's Not Important

If you've never suffered the effects of data loss, you might not realize the catastrophic consequences that can result. In some cases, it can lead to the demise of a business! Without backup, a business might have to curtail operations until data is restored, something from which the business might never recover financially. With backup and the ability to quickly restore lost files, a business can continue to thrive without skipping a beat.

Excuse #6: It Won't Happen to Me

Data loss events happen more frequently than you'd like to think. They can be the result of human error, natural disasters, theft, viruses, hardware failure—all can result in the loss of data. Having automatic, continuous backup is like insurance you buy, hoping you'll never need it, but you're relieved to have it when (not if) something unfortunate happens.

Excuse #7: I Forgot!

Although there are numerous backup solutions that require users to manually maintain, there are also others that are automatic and continuous. These allow SMBs to focus on their business, not on remembering to back up their data.

Excuse #8: It's Too Complicated

Although this might have been the case in the "old days," when backup required tape and complicated schemes for backing up the backup and for testing and verifying the backup archive, it's certainly no longer true. Today, backup solutions can be set up quickly, with no technical expertise required, and then forgotten about. For the most part, SMBs can even restore all by themselves without a call to the Help desk or a backup service to get their files back.

Excuse #9: I'll Just Use a Data Recovery Service if Things Crash

Data recovery services are useful only when you have a computer to recover. They're no use at all if your laptop is lost or stolen. Also, these services are notoriously expensive, with no guarantees that all, if any, of your data will be recovered. And how will your business limp along without your files in the weeks it could take to get your files back? Why chance it?

Excuse #10: I Copy Files to a Thumb Drive

Copying isn't the same a backing up (it's much more cumbersome and is an inefficient use of storage). Also, if something happens to that drive, it's as if you never backed up at all. That's why there are backup solutions that offer the ability to back up online (for secure offsite protection) and to local drives (for rapid restores).

—Jason Bovberg

InstantDoc ID 140893

PowerShell: The Gift That Keeps On Giving to Microsoft Exchange Server

I realize that many administrators who work with Microsoft Exchange Server might not share my enthusiasm for PowerShell. After all, isn't revisiting the command line something that makes one think that you're coping with the piping and scripting loved by UNIX and Linux geeks? Well, Windows PowerShell's command-line nature is there for all to see, and PowerShell is awfully fond of piping (and gets a lot of its power from this ability). Also, there's no doubt that scripting is something that PowerShell devotees spend a lot of their time discussing.

But all of this is missing the point. The reason I think PowerShell has made such a contribution to Exchange is simple: PowerShell provides the ability to automate common administrative tasks quickly, simply, and accurately in a way that even the best-designed GUI-based management console will never be able to do.

The Exchange development group took the momentous decision from Exchange Server 2007 onward to encapsulate the business logic that drives the product around its very large set of 600+ PowerShell cmdlets. In passing, let me say that "cmdlet" is one of my least favorite technical terms. I would much prefer the simplicity of the term"command" instead. However, cmdlet is the term coined by PowerShell developers—and who am I to debate the wisdom of their choice?

Moving away from my bias against cmdlet (only the term, not the implementation), the decision taken for Exchange 2007 let developers build Exchange administrative interfaces on a common foundation, meaning that the Exchange Management Console (EMC), the setup program, and the Exchange Management Shell (EMS) all execute the same code. This eliminated the inconsistency seen in previous versions of Exchange and let Microsoft remove redundant and overlapping code.

The central role of PowerShell was further expanded in Exchange Server 2010 with the addition of the Exchange Control Panel (ECP), which leverages the same platform as EMC and EMS. Exchange 2010 also ties its Role-Based Access Control (RBAC) mechanism to its PowerShell cmdlets, defining roles in terms of the cmdlets that a holder of a role can execute. Indeed, the granularity is such that RBAC lets roles define the level of parameters to a cmdlet that a user can execute, meaning that users can retrieve details of their mailboxes (running the Get-Mailbox cmdlet behind the scenes) and set some properties (with Set-Mailbox), whereas administrators can do a lot more.

Exchange 2010 also includes remote PowerShell that lets administrators run PowerShell to manage remote Exchange servers from workstations and other computers. Remote PowerShell forces users to connect via IIS and be authenticated to build a session that connects to Exchange. The session includes details of the cmdlets and parameters that the user is entitled to use as defined by the RBAC roles that they hold. Collectively, these components provide the ability to connect to Exchange Online running in Office 365 to perform management using the EMC, ECP, or EMS. Indeed, as explained in "How to Manage Your Exchange 2010 Organization with PowerShell Implicit Reporting over the Internet" (http://bit.ly/mRz6x4), it's even possible to emulate the connections used to connect with PowerShell to manage Office 365 by establishing external connections from the Internet to manage on-premises Exchange 2010 servers (protected of course by a reverse proxy).

There's no doubt that the move to comprehensively embrace PowerShell was a stunning and far-reaching decision that no other major Microsoft server product emulated for several years. Indeed, it's only recently that elements of Windows Server have supported similar access via PowerShell. Perhaps the biggest breakthrough will occur in Windows 8, because Windows Server 8's GUI-based management console is built on top of PowerShell. The most important points are that Windows Server 8 contains hundreds of new cmdlets to enable management of components from the shell and to eliminate the need for administrators to use GUI consoles. In short, Windows administrators need to get rid of the idea of logging on to a server to do work, something that Exchange administrators have become used to since the advent of remote PowerShell support in Exchange 2010.

In addition, the developer preview of Windows Server 8 includes PowerShell Web Access, another component of PowerShell 3.0. To me, PowerShell Web Access looks very much like a natural development from the ideas proven by Exchange 2010's implementation of remote PowerShell where servers are managed from workstations through PowerShell without the need to log on directly to the target server. The interaction between workstation and target server is managed by a combination of IIS, Active Directory (AD), and Exchange's RBAC security model.

All in all, PowerShell provides Exchange administrators with huge potential for managing their servers in a way that the EMC or ECP just can't deliver. In passing, let me also acknowledge the wisdom of whoever decided to include the function into the EMC that outputs the PowerShell code for the different operations performed through the console; this is a fantastic learning device for anyone who wants to understand the basic syntax and construct for using PowerShell to manage Exchange. If you haven't yet taken the plunge to get down and dirty with PowerShell, you're really missing out on something that can save you scads of time.

—Tony Redmond

InstantDoc ID 140470

Mobile Device Management in the BYOD World

How important is mobile device management to your business? We've gone beyond the days when organizations could simply standardize on a single device or platform, such as BlackBerry, and manage everything the same. It's not even just iPhone or Android smartphones anymore; the iPad has launched the tablet space in earnest. The BYOD world has taken over.

I'm not saying that BYOD is necessarily a bad thing. If you can increase employee satisfaction and effectiveness by letting them use the mobile devices they love best, it seems like an easy win—provided your IT department is prepared to manage the variety of devices such a situation brings. Because most devices these days can be managed through Microsoft's Exchange ActiveSync (EAS) protocol, IT shops at least have an avenue of control.

In a recent non-scientific Instant Poll on the Exchange & Outlook page of WindowsITPro.com, I posed the question, "How concerned are you about the security (both physical—loss or damage—and malware) of mobile devices your organization supports?"

Here are the results from my informal *Windows IT Pro* Exchange & Outlook reader survey:

- 35% of our readers are very concerned
- 47% of our readers are somewhat concerned
- 12% of our readers are somewhat unconcerned
- 6% of our readers are not at all concerned

Clearly, mobile device security is on the mind of the majority of IT pros out there. The next logical question is: What are you doing to protect those devices and your networks?

In fact, according to Paul DePond, president and founder of mobile device management (MDM) vendor Notify Technology, this is the number-one topic around mobility that's being discussed in companies that aren't standardized on BlackBerry. As DePond said, when it comes to MDM, companies come in three flavors: "Those who needed it yesterday, those who need it now, and those who are going to get to it."

MDM isn't just about guarding against malware entering your network and the careless employee who drops his smartphone in the toilet (and then probably reports it as lost or stolen to avoid embarrassment). You also have to be aware that employees have the capability to carry around vast amounts of corporate data in their pockets. You need to be able to apply corporate policies to data on those devices just as you would on a desktop PC—particularly if you're in a highly regulated industry.

"Remember when we called them rogue devices?" Julie Palen said. Palen is the senior vice president of MDM for Tangoe. "Now there's more rogue devices than there are managed devices, and those rogue devices are coming from all levels of the organization." When it comes to understanding the size of the problem, Palen said, "Probably 25 percent of companies really get it, and 75 percent are going to get it. We see an awful lot of companies planning and figuring it out."

Tangoe and Notify Technology are just two of the many companies offering MDM solutions these days. Larger companies are going to find more benefits from investing in a third-party solution for MDM than will smaller organizations. But certainly almost every organization by this point should be working on its strategy for this difficult topic. Mobile device proliferation continues to grow. And as Palen said, "As you start to hear more stories about companies and their challenges, you're going to have other companies say, 'Wait, I've got to figure this out while it's a 300-device problem, before it's a 13,000-device problem."

—B.K. Winstead

InstantDoc ID 140841

SavvyAssistants
Your guide to sponsored resources

Are you following us?
Windows IT Pro is on Twitter! Follow @WindowsITPro for the latest news and articles, and @SavvyAsst for helpful resources, free tools, new events, and industry happenings. Check us out!
windowsitpro.com/go/Twitter

Don't be a stranger - become a friend!
The Windows IT Pro community is the heartbeat of the Windows IT world—a gathering of people, content and resources focused on Microsoft Windows technologies and applications. It's a "community" in every sense, bringing an independent, uncensored voice to IT managers, network and systems administrators, developers, systems analysts, CIOs, CTOs, and other technologists at companies worldwide. And we're on Facebook. Join us and stay connected with the IT world!
windowsitpro.com/go/Facebook

Get the latest updates on upcoming events and popular resources
Join our LinkedIn network to get real-time updates on news, events, and related resources!
windowsitpro.com/go/LinkedIn



AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the websites listed below.

1&1 Internet 61
www.1and1.com

Altova 70, 71
www.altova.com

APC/Schneider Electric Cover 3
www.apc.com/promo

AvePoint 38, 39
www.avepoint.com

Axceler 50, 51
www.axceler.com

Cisco 62, 63
www.cisco.com/go/microsoft

Devfarm Software 11
www.powerwf.com

Diskeeper Corporation 47, 49
www.diskeeper.com

HP 18, 19
www.hp.com/go/e5000

IBM Corporation Cover 2, 5
www.ibm.com/facts

IBM Corporation 33
www.ibm.com/systems/reliability

Microsoft Cover 4
www.microsoft.com/office365

NetWrix 14, 15
www.netwrix.com

Paul Thurrott Mobile App 37
www.windowsitpro.com/mobile-apps

Penton Marketing Services 66
www.pentonmarketingservices.com

SharePoint Virtual Conference 3
www.sharepointpromag.com/events

TrainSignal 80, 81
www.trainsignal.com

VMware 28, 29
www.vmware.com

WinConnections Spring 2012 Event .. Cover tip, 6
www.WinConnections.com

Windows IT Pro e-Learning Series 52
http://elearning.left-brain.com

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

A10 Networks 27
Acronis 25
Altova 30
AppAssure 30, 25
Apple 8, 26, 32, 83
ARCHOS 82
Automation Anywhere 35
AvePoint 25
Axceler 34
BA Insight 34
Barracuda Networks 27
Blackbird Group 24
CA 30
CBT Nuggets 36
Centrify 24, 30, 34
Cisco Systems 27
Citrix Systems 36
Code 42 Software 84
CommVault 25, 30
Comodo 24
DataCore 36
Dell 26, 27, 36
Devfarm Software 34
Diskeeper 35
Drobo 27
Dropbox 25
EMC 27
ENow 31
ESET 24
F5 Networks 27
GFI Software 32, 83
Google 25, 32, 36
HP 26, 27, 31, 35, 36
IBM 26, 31
Idera 34
Imanami 24
Juniper Networks 27
Lenovo 26
Lieberman Software 34
LogLogic 83
LogMeIn 32, 35, 36
Malwarebytes 34
ManageEngine 24, 25, 32, 35
McAfee 24
Mountain View Systems 36
NetApp 27
NETIKUS.NET 32
NetIQ 35
NETsec 30
Network Automation 24, 30, 31, 34, 35, 36
Network Instruments 83
NetWrix 35
Notepad++ 36
Paragon Software 30, 35
Qualys 34
Quest Software 24, 30, 32, 34, 82
Rackspace 25
RealVNC 30
RIM 8
SAPIEN Technologies 34
ScriptLogic 25
Shavlik Technologies 32
Skype 31, 36
Skytap 30
Snort 35
SolarWinds 32, 36
Specops Software 34
Spiceworks 30, 36
StorSimple 27
Symantec 24, 25, 27, 30, 32, 34
TITUS 34
TrainSignal 36
Transcender 36
Transend 31
up.time software 82
Veeam 25, 30
Visage Mobile 82
VMware 24, 25, 30, 32, 36
XIO 27
Zenprise 32

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

DevProConnections UPDATE
Exchange & Outlook UPDATE
Security UPDATE
SharePoint Pro UPDATE
SQL Server Magazine UPDATE
Windows IT Pro UPDATE
WinInfo Daily UPDATE
www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles:
penton@wrightsmedia.com

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the web. Includes FREE access to eBooks and archived eLearning events, plus a subscription to either *Windows IT Pro* or *SQL Server Magazine*.
www.windowsitpro.com/go/vipsub

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro



Ctrl+Alt+Del

by Jason Bovberg

"Send your funny screenshots, oddball product news, and hilarious end-user stories to rumors@windowsitpro.com. If we use your submission, you'll receive a *Windows IT Pro* Rubik's Cube."

Top 25 Most Ridiculous End-User Questions

In our 2011 *Windows IT Pro* Community Choice survey, we took the opportunity to ask you some lighthearted questions about your job. You'll see some of those findings throughout our awards coverage toward the front of this magazine. But we left one particular question for the back page. Here's a collection of your responses to the question, "What's the most ridiculous question you've received from an end user?"

1. "Can you answer a quick question?"
2. "Is the Internet broken?"
3. "Is my keyboard wireless?"
4. "What's the admin password?"
5. "How do I undo something I don't remember doing?"
6. "How do I right-click the mouse?"
7. "When is the power coming back on?" (during a power outage)
8. "My monitor just died. Is it plugged in? I can't tell because the lights went out."
9. "The printer isn't working. Can you look at it?" (The printer was out of paper.)
10. "How do I open a file?"
11. "Is your phone working?"
12. "I forgot my file on my other computer. Can you set up a server so I can get it?"
13. "Can you unblock YouTube so I can watch it during lunch?"
14. "The email you sent me went to my spam folder. Can you send it again?"
15. "What's my username?" (after 15 years of logging on with the same account)
16. "Why does my computer smell bad?"
17. "Why can't I just print out all my mail?"
18. "How do you make a smiley face in Microsoft Word?"
19. "Can you please reboot the Yahoo! server?"
20. "How fast is 1MBps?"
21. "My blue thing won't come on."
22. "Why doesn't the error message tell me what to do to fix the problem?"
23. "How do I download the Internet to my computer?"
24. "I accidentally deleted the Internet, can you help?" (after removing the IE 8 shortcut from the desktop)
25. "Excuse me, are you busy?"

USER MOMENT OF THE MONTH

I was working on a Level 1-3 Help desk and got a call from a user, who said that his site was shutting down for four hours because the local power company needed to perform some maintenance. So, I gracefully shut down the servers. One hour later, the same user called back and said that he couldn't access his applications. "Well," I said, "that's because the servers were shut down. Someone needs to power them back up." He responded, "Oh, do servers require power?"

—Chris

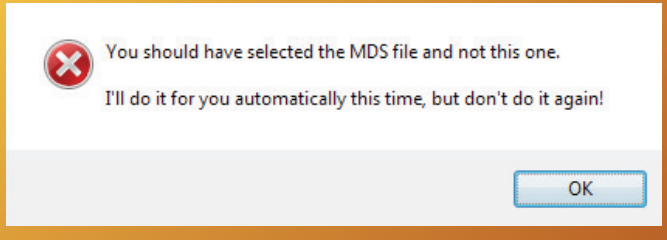


Figure 1: Be warned!

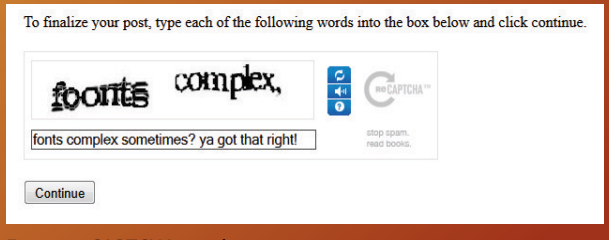


Figure 2: CAPTCHA gotcha

December 2011 issue no. 208, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Copyright 2011, Penton Media, Inc., all rights reserved. Windows is a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries, and *Windows IT Pro* is used under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation. Microsoft Corporation is not responsible in any way for the editorial policy or other contents of the publication. *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 748 Whalers Way, Fort Collins, CO 80525. Advertising rates furnished upon request. Periodicals Class postage paid at Fort Collins, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,*** 748 Whalers Way, Fort Collins, CO 80525. **SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 748 Whalers Way, Fort Collins, CO 80525. Printed in the USA.

Now, deploy your IT whenever and wherever you need it.



APC by Schneider Electric helps you upgrade IT capabilities without overhauling space.

Is your lack of IT space a barrier to adopting new technologies?

Consolidation, virtualization, network convergence, blade servers—these new technologies improve efficiency, cut costs, and allow you to "do more with less." But they also bring power, cooling, and management challenges, especially when you're tasked with deploying your IT without dedicated space. You're relying on guesswork, depending on building air conditioning, or improvising remedies. So, how can you increase the level of reliability and control of your server deployment without spending a fortune?

The availability you need—without the IT room.

APC by Schneider Electric™ understands the challenges of delicately matching IT needs with logistical realities. Fortunately, we have adaptable and flexible solutions that provide everything for your IT deployment: reliable and efficient power, cooling, monitoring, and management. Whatever your logistical or space constraints, we have a total solution to meet your specific needs. All components have been pre-engineered to work together and integrate seamlessly with your existing equipment.

Future-proof your IT deployment.

There's no need for confusing cooling configurations or expensive mechanical re-engineering, so our modular, "pay-as-you-grow" designs let you be 100 percent confident that your IT capabilities can keep pace with ever-changing demands. Self-contained cooling, high-density enclosures, rack-level power distribution and monitoring sensors, and integrated management software provide complete remote control and unprecedented visibility into your entire IT system. Simply add power protection (such as undisputed, best-in-class Smart-UPS™ or Symmetra™ units), and you have a total solution for today, tomorrow, and beyond.

InfraStruxure



1. **Enclosures** Vendor-neutral NetShelter™ SX rack design handles high-density airflow and power needs.
2. **Power** Ultra-reliable Smart-UPS and Symmetra UPS offer scalable runtime, and PDUs are rack-mounted.
3. **Environmental monitoring and management** PoE-enabled temperature sensors let you keep an eye on conditions at the rack level, and centralized software gives you real-time insight into the entire system.



The NetShelter CX Office enclosure is available in three sizes: 18U, 24U and 38U.

Expand your IT capabilities without building out.

The unique, soundproof, self-contained NetShelter CX enclosure solution includes everything you need to house a highly reliable IT deployment regardless of space limitations.



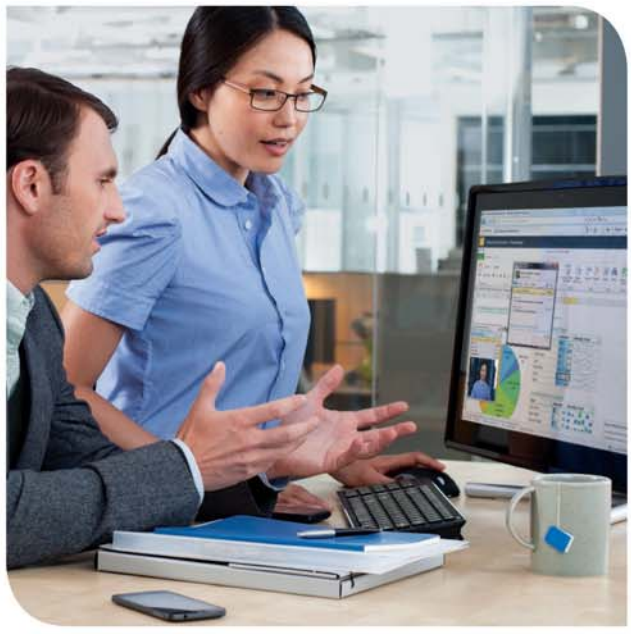
Learn how to reduce cooling expenses with our FREE Cooling Efficiency kit and enter to win 1 of 5 Smart-UPS units (SMX1000)!

Visit www.apc.com/promo Key Code j561v • Call 888-289-APCC x6320 • Fax 401-788-2797

APC™ by Schneider Electric

©2011 Schneider Electric. All Rights Reserved. Schneider Electric, APC, Smart-UPS, Symmetra, InfraStruxure, and NetShelter are trademarks owned by Schneider Electric Industries SAS or its affiliated companies. email: esupport@apc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA • 998-4722_GMA-GB

Microsoft









Streamlined provisioning.
Easy-to-use permissions.
Enterprise-grade security.
It all works together.

Introducing Microsoft Office 365. Collaborate in the cloud with Office, Exchange, SharePoint, and Lync videoconferencing. **Starting as low as $10 per user per month. Begin your free trial now at Microsoft.com/office365**

Scan tag with a smartphone to learn about the Office 365 free trial.
Download the free scanner app at http://gettag.mobi

Microsoft® Office 365